Accountability and Access Control

THE CISSP EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE:

✓ Accountability
✓ Access Control Techniques
✓ Access Control Administration
✓ Identification and Authentication Techniques
✓ Access Control Methodologies and Implementation
The Access Control Systems and Methodology domain of the Common Body of Knowledge (CBK) for the CISSP certification exam deals with topics and issues related to the monitoring, identification, and authorization of granting or restricting user access to resources. Generally, an access control is any hardware, software, or organizational administrative policy or procedure that grants or restricts access, monitors and records attempts to access, identifies users attempting to access, and determines whether access is authorized.

In this chapter and in Chapter 2, “Attacks and Monitoring,” the Access Control Systems and Methodology domain is discussed. Be sure to read and study the materials from both chapters to ensure complete coverage of the essential material for this domain of the CISSP certification exam.

Access Control Overview

Controlling access to resources is one of the central themes of security. Access control addresses more than just controlling which users can access which files or services. Access control is about managing how subjects interact with objects. The transfer of information from an object to a subject is called access. Subjects are active entities that, through the exercise of access, seek information about or data from passive entities, or objects. A subject can be a user, program, process, file, computer, database, and so on. An object can be a file, database, computer, program, process, file, printer, storage media, and so on. The subject is always the entity that receives information about or data from the object. The subject is also the entity that alters information about or data stored within the object. The object is always the entity that provides or hosts the information or data. The roles of subject and object can switch as two entities, such as a program and a database or a process and a file, communicate to accomplish a task.

Types of Access Control

Access controls are necessary to protect the confidentiality, integrity, and availability of objects (and by extension, their information and data). The term access control is used to describe a broad range of controls, from forcing a user to provide a valid username and password to log on to preventing users from gaining access to a resource outside of their sphere of access.

Access controls can be divided into the following seven categories of function or purpose. You should notice that some security mechanisms can be labeled with multiple function or purpose categories.
CIA Triad

The essential security principles of confidentiality, integrity, and availability are often referred to as the CIA Triad. All security controls must address these principles. These three security principles serve as common threads throughout the CISSP CBK. Each domain addresses these principles in unique ways, so it is important to understand them both in general terms and within each specific domain:

- Confidentiality is the principle that objects are not disclosed to unauthorized subjects.
- Integrity is the principle that objects retain their veracity and are intentionally modified by authorized subjects only.
- Availability is the principle that authorized subjects are granted timely access to objects with sufficient bandwidth to perform the desired interaction.

Different security mechanisms address these three principles in different ways and offer varying degrees of support or application of these principles. Objects must be properly classified and prioritized so proper security access controls can be deployed. These and many other issues related to the CIA Triad are discussed throughout this book.

Preventative access control  A preventative access control is deployed to stop unwanted or unauthorized activity from occurring. Examples of preventative access controls include fences, locks, biometrics, mantraps, lighting, alarm systems, separation of duties, job rotation, data classification, penetration testing, access control methods, encryption, auditing, smart cards, callback, security policies, security awareness training, and antivirus software.

Detective access control  A detective access control is deployed to discover unwanted or unauthorized activity. Examples of detective access controls include security guards, guard dogs, motion detectors, security cameras, job rotation, mandatory vacations, audit trails, supervision of users, incident investigations, and intrusion detection systems.

Corrective access control  A corrective access control is deployed to restore systems to normal after an unwanted or unauthorized activity has occurred. Examples of corrective access controls include intrusion detection systems, antivirus solutions, alarms, mantraps, and security policies. Corrective controls have only a minimal capability to respond to access violations.

Deterrent access control  A deterrent access control is deployed to discourage the violation of security policies. Examples of deterrent access controls include locks, fences, security badges, security guards, mantraps, security cameras, trespass or intrusion alarms, separation of duties, work task procedures, awareness training, encryption, auditing, and firewalls.

Recovery access control  A recovery access control is deployed to repair or restore resources, functions, and capabilities after a violation of security policies. Examples of recovery access controls include backups, fault tolerant drive systems, server clustering, antivirus software, and
database shadowing. Recovery controls have a more advanced or complex capability to respond to access violations than a corrective access control. For example, a recovery access can repair damage as well as stop further damage.

**Compensation access control**  A compensation access control is deployed to provide various options to other existing controls to aid in the enforcement and support of a security policy. Examples of compensation access controls include security policy, personnel supervision, monitoring, and work task procedures.

**Directive access control**  A directive access control is deployed to direct, confine, or control the actions of subjects to force or encourage compliance with security policies. Examples of directive access controls include security guards, guard dogs, security policy, monitoring, supervising, work task procedures, and awareness training.

Access controls can be further categorized by how they are implemented. In this case, the categories are administrative, logical/technical, or physical:

**Administrative access controls**  Administrative access controls are the policies and procedures defined by an organization’s security policy to implement and enforce overall access control. Administrative access controls focus on two areas: personnel and business practices. Examples of administrative access controls include policies, procedures, hiring practices, background checks, data classification, security training, vacation history, reviews, work supervision, personnel controls, and testing.

**Logical/technical access controls**  Logical access controls and technical access controls are the hardware or software mechanisms used to manage access to resources and systems and provide protection for those resources and systems. Examples of logical or technical access controls include encryption, smart cards, passwords, biometrics, constrained interfaces, access control lists (ACLs), protocols, firewalls, routers, intrusion detection systems, and clipping levels.

**Physical access controls**  Physical access controls are the physical barriers deployed to prevent direct contact with systems or portions of a facility. Examples of physical access controls include guards, fences, motion detectors, locked doors, sealed windows, lights, cable protection, laptop locks, swipe cards, guard dogs, video cameras, mantraps, and alarms.

### Access Control in a Layered Environment

No single access control mechanism is ever deployed on its own. In fact, combining various types of access controls is the only means by which a reasonably secure environment can be developed. Often multiple layers or levels of access controls are deployed to provide layered security or defense in depth. This idea is described by the notion of concentric circles of protection, which puts forth the concept of surrounding your assets and resources with logical circles of security protection. Thus, intruders or attackers would need to overcome multiple layers of defenses to reach the protected assets.

In a layered security or concentric circles of protection deployment, your assets are surrounded by a layer of protection provided for by administrative access controls, which in turn is surrounded by a layer of protection consisting of logical or technical access controls, which
Access Control Overview

is finally surrounded by a layer of protection that includes physical access controls. This concept of defense in depth highlights two important points. First, the security policy of an organization ultimately provides the first or innermost layer of defense for your assets. Without a security policy, there is no real security that can be trusted. Security policies are one element of administrative access controls. Second, people are your last line of defense. People or personnel are the other focus of administrative access control. Only with proper training and education will your personnel be able to implement, comply with, and support the security elements defined in your security policy.

The Process of Accountability

One important purpose of security is to be able to hold people accountable for the activities that their online personas (i.e., their user accounts) perform within the digital world of the computer network. The first step in this process is identifying the subject. In fact, there are several steps leading up to being able to hold a person accountable for online actions: identification, authentication, authorization, auditing, and accountability.

Identification

Identification is the process by which a subject professes an identity and accountability is initiated. A user providing a username, a logon ID, a personal identification number (PIN), or a smart card represents the identification process. Providing a process ID number also represents the identification process. Once a subject has identified itself, the identity is accountable for any further actions by that subject. Information technology (IT) systems track activity by identities, not by the subjects themselves. A computer doesn’t know one human from another, but it does know that your user account is different from all other user accounts.

Authentication

Authentication is the process of verifying or testing that the claimed identity is valid. Authentication requires that the subject provide additional information that must exactly correspond to the identity indicated. The most common form of authentication is a password, which falls under the first of three types of information that can be used for authentication:

Type 1 A Type 1 authentication factor is something you know, such as a password, personal identification number (PIN), lock combination, pass phrase, mother’s maiden name, favorite color, and so on.

Type 2 A Type 2 authentication factor is something you have, such as a smart card, token device, memory card, and so on. This can also include your physical location, referred to as the “somewhere you are” factor.

Type 3 A Type 3 authentication factor is something you are, such as fingerprints, voice print, retina pattern, iris pattern, face shape, palm topology, hand geometry, and so on.

In addition to these three commonly recognized factors, there are at least two others. One is called “something you do,” such as writing a signature, typing out a pass phrase (keyboard
dynamics), or saying a phrase. Something you do is often included in the “something you are” category. Another factor, mentioned earlier, is called “somewhere you are,” such as the computer terminal from which you logged in or the phone number (identified by caller ID) or country (identified by your IP address) from which you dialed up. Somewhere you are is often included in the “something you have” category.

**Two-factor authentication** occurs when two different factors are required to provide authentication. For example, when cashing a check at the grocery store, you often have to provide your driver’s license (something you have) and your phone number (something you know). Strong authentication is simply any authentication that requires two or more factors but not necessarily different factors. However, as a general rule, when different factors are employed, the resultant authentication is more secure.

Once the *logon credentials* of the offered identity and the authentication factor(s) are provided to the system, they are checked against the database of identities on the system. If the identity is located and the correct authentication factor(s) have been provided, then the subject has been authenticated.

**Authorization**

Once a subject is authenticated, its access must be authorized. The process of *authorization* ensures that the requested activity or object access is possible given the rights and privileges assigned to the authenticated identity (which we will refer to as the subject from this point forward). In most cases, the system evaluates an *access control matrix* that compares the subject, the object, and the intended activity (we discuss the access control matrix in greater detail in Chapter 11 “Principles of Computer Design”). If the specific action is allowed, the subject is authorized. If the specific action is not allowed, the subject is not authorized.

Keep in mind that just because a subject has been identified and authenticated, it does not automatically mean they have been authorized. It is possible for a subject to be logged onto a network (i.e., identified and authenticated) but blocked from accessing a file or printing to a printer (i.e., by not being authorized to perform that activity). Most network users are authorized to perform only a limited number of activities on a specific collection of resources. Identification and authentication are “all or nothing” aspects of access control. Authorization has a wide range of variations between all and nothing for each individual subject or object within the environment. A user may be able to read a file but not delete it. A user may be able to print a document but not alter the print queue. A user may be able to log onto a system but not access any resources.

It is important to understand the differences between identification, authentication, and authorization. Although they are similar and are essential to all security mechanisms, they are distinct and must not be confused.

**Auditing and Accountability**

Auditing is the process by which the online activities of user accounts and processes are tracked and recorded. Auditing produces audit trails. Audit trails can be used to reconstruct events and to verify whether or not security policy or authorization was violated. By comparing the contents of audit trails with authorization against authenticated user accounts, the people associated with user accounts can be held accountable for the online actions of those user accounts.
An organization’s security policy can be properly enforced only if accountability is maintained. In other words, security can be maintained only if subjects are held accountable for their actions. Effective accountability relies upon the capability to prove a subject’s identity and track their activities. Thus, accountability builds on the concepts of identification, authentication, authorization, access control, and auditing.

Identification and Authentication Techniques

Identification is a fairly straightforward concept. A subject must provide an identity to a system to start the authentication, authorization, and accountability processes. Providing an identity can be typing in a username, swiping a smart card, waving a token device, speaking a phrase, or positioning your face, hand, or finger for a camera or scanning device. Without an identity, a system has no way to correlate an authentication factor with the subject. A subject’s identity is typically considered to be public information.

Authentication verifies the identity of the subject by comparing one or more factors against the database of valid identities (i.e., user accounts). The authentication factor used to verify identity is typically considered to be private information. The ability of the subject and system to maintain the secrecy of the authentication factors for identities directly reflects the level of security of that system.

Identification and authentication are always together as a single two-step process. Providing an identity is step one and providing the authentication factor(s) is step two. Without both, a subject cannot gain access to a system—neither element alone is useful.

There are several types of authentication information a subject can provide (e.g., something you know, something you have, etc.). Each authentication technique or factor has its unique benefits and drawbacks. Thus it is important to evaluate each mechanism in light of the environment in which it will be deployed to determine viability.

Passwords

The most common authentication technique is the use of passwords, but they are also considered to be the weakest form of protection. Passwords are poor security mechanisms for several reasons, including the following:

- Users typically choose passwords that are easy to remember and therefore easy to guess or crack.
- Randomly generated passwords are hard to remember, thus many users write them down.
- Passwords are easily shared, written down, and forgotten.
- Passwords can be stolen through many means, including observation, recording and playback, and security database theft.
8  Chapter 1 • Accountability and Access Control

- Passwords are often transmitted in cleartext or with easily broken encryption protocols.
- Password databases are often stored in publicly accessible online locations.
- Short passwords can be discovered quickly in brute force attacks.

Password Selection

Passwords can be effective if selected intelligently and managed properly. There are two types of passwords: static and dynamic. Static passwords always remain the same. Dynamic passwords change after a specified interval of time or use. One-time passwords or single-use passwords are a variant of dynamic passwords that are changed every time they are used. One-time passwords are considered the strongest type of password. As the importance of maintaining security increases, so does the need to change passwords more frequently. The longer a password remains static and the more often the same password is used, the more likely it will be compromised or discovered.

In some environments, the initial passwords for user accounts are automatically generated. Often the generated password is a form of composition password. A composition password is a password constructed from two or more unrelated words joined together with a number or symbol in between. Composition passwords are easy for computers to generate, but they should not be used for extended periods of time because they are vulnerable to password guessing attacks.

A password mechanism that is slightly more effective than a basic password is a pass phrase. A pass phrase is a string of characters usually much longer than a password. Once the pass phrase is entered, the system converts it into a virtual password for use by the authentication process. Pass phrases are often modified natural language sentences to allow for simplified memorization. Here’s an example: “She $ell$ C shells ByE the c-shor.”

Another interesting password mechanism is the cognitive password. A cognitive password is usually a series of questions about facts or predefined responses that only the subject should know. For example, three to five questions might be asked of the subject, such as the following:

- What is your birth date?
- What is your mother’s maiden name?
- What is the name of your division manager?
- What was your score on your last evaluation exam?
- Who was your favorite baseball player in the 1984 World Series?

If all the questions are answered correctly, the subject is authenticated. The most effective cognitive password systems ask a different set of questions each time. The primary limitation of cognitive password systems is that each question must be answered at the time of user enrollment (i.e., user account creation) and answered again during the logon process, which increases the time to log on.

Many systems include password policies that restrict or dictate the characteristics of passwords. Common restrictions are minimum length, minimum age, maximum age, requiring three or four character types (i.e., uppercase, lowercase, numbers, symbols), and preventing password reuse. As the need for security increases, these restrictions should be tightened.

However, even with strong software-enforced password restrictions, easily guessed or cracked passwords can still be created. An organization’s security policy must clearly define
both the need for strong passwords and what a strong password is. Users need to be trained about security so they will respect the organization’s security policy and adhere to its requirements. If passwords are created by end users, offer suggestions such as the following for creating strong passwords:

- Don’t reuse part of your name, logon name, e-mail address, employee number, Social Security number, phone number, extension, or other identifying name or code.
- Don’t use dictionary words, slang, or industry acronyms.
- Do use nonstandard capitalization and spelling.
- Do switch letters and replace letters with numbers.

**Password Security**

When a malicious user or attacker seeks to obtain passwords, there are several methods they can employ, including network traffic analysis, password file access, brute force attacks, dictionary attacks, and social engineering. Network traffic analysis (also known as sniffing) is the process of capturing network traffic when a user is entering a password for authentication. Once the password is discovered, the attacker attempts to replay the packet containing the password against the network to gain access. If an attacker can gain access to the password database file, it can be copied and a password cracking tool can be used against it to extract usernames and passwords. Brute force and dictionary attacks are types of password attacks that can be waged against a stolen password database file or a system’s logon prompt. In a dictionary attack, the attacker uses a script of common passwords and dictionary words to attempt to discover an account’s password. In a brute force attack, a systematic trial of all possible character combinations is used to discover an account’s password. A social engineering attack is an attempt by an attacker to obtain logon capabilities through deceiving a user, usually over the telephone, into performing specific actions on the system, such as changing the password of an executive who’s on the road or creating a user account for a new fictitious employee.

There are several ways to improve the security of passwords. Account lockout is a mechanism used to disable a user account after a specified number of failed logons occur. Account lockouts stop brute force and dictionary attacks against a system’s logon prompt. Once the logon attempt limit is reached, a message displaying the time, date, and location (i.e., computer name or IP address) of the last successful or failed logon attempt is displayed. Users who suspect that their account is under attack or has been compromised can report this to the system administrator. Auditing can be configured to track logon success and failure. An intrusion detection system can easily identify logon prompt attacks and notify administrators.

There are other options to improve the security offered by password authentication:

- Use the strongest form of one-way encryption available for password storage.
- Never allow passwords to be transmitted over the network in cleartext or with weak encryption.
- Use password verification tools and password cracking tools against your own password database file. Require that weak or discovered passwords be changed.
Chapter 1 • Accountability and Access Control

- Disable user accounts for short periods of inactivity, such as a week or a month. Delete user accounts that are no longer used.
- Properly train users about the necessity of maintaining security and the use of strong passwords. Warn about writing down or sharing passwords. Offer tips to prevent shoulder surfing or keyboard logging to capture passwords. Offer tips and recommendations on how to create strong passwords.

Biometrics

Another common authentication and identification technique is the use of biometric factors. Biometric factors fall into the “something you are” authentication category. A biometric factor is a behavioral or physiological characteristic that is unique to a subject. There are many types of biometric factors, including fingerprints, face scans, iris scans, retina scans, palm scans (also known as palm topography or palm geography), heart/pulse patterns, voice patterns, signature dynamics, and keystroke patterns.

Biometric factors can be used as an identifying or authentication technique. Using a biometric factor instead of a username or account ID as an identifier requires a one-to-many search of the offered biometric pattern against the stored database of patterns. As an identification technique, biometric factors are used in physical access controls. Using a biometric factor as an authentication technique requires a one-to-one match of the offered biometric pattern against the stored pattern for the offered subject identity. As an authentication technique, biometric factors are used in logical access controls.

The use of biometrics promises universally unique identification for every person on the planet. Unfortunately, biometric technology has yet to live up to this promise. For biometric factors to be useful, they must be extremely sensitive. The most important aspect of a biometric device is its accuracy. To use biometrics as an identifying mechanism, a biometric device must be able to read information that is very minute, such as the variations in the blood vessels in a person’s retina or the tones and timbres in their voice. Because most people are basically similar, the level of detail required to authenticate a subject often results in false negative and false positive authentications.

Biometric Factor Ratings

Biometric devices are rated for their performance against false negative and false positive authentication conditions. Most biometric devices have a sensitivity adjustment so they can be tuned to be more or less sensitive. When a biometric device is too sensitive, a Type 1 error occurs. A Type 1 error occurs when a valid subject is not authenticated. The ratio of Type 1 errors to valid authentications is known as the False Rejection Rate (FRR). When a biometric device is not sensitive enough, a Type 2 error occurs. A Type 2 error occurs when an invalid subject is authenticated. The ratio of Type 2 errors to valid authentications is known as the False Acceptance Rate (FAR).

The FRR and FAR are usually plotted on a graph that shows the level of sensitivity adjustment against the percentage of FRR and FAR errors (see Figure 1.1). The point at which the FRR and FAR are equal is known as the Crossover Error Rate (CER). The CER level is used as a standard assessment point from which to measure the performance of a biometric device. In some situations, having a device more sensitive than the CER rate is preferred, such as with a metal detector at an airport.
Biometric Registration

In addition to the sensitivity issues of biometric devices, there are several other factors that may cause them to be less than effective—namely, enrollment time, throughput rate, and acceptance. For a biometric device to function as an identification or authentication mechanism, the subject must be enrolled or registered. This means the subject’s biometric factor must be sampled and stored in the device’s database. The time required to scan and store a biometric factor varies greatly by what physical or performance characteristic is used. The longer it takes to enroll with a biometric mechanism, the less a user community accepts the inconvenience. In general, enrollment times longer than two minutes are unacceptable. If you use a biometric characteristic that changes with time, such as a person’s voice tones, facial hair, or signature pattern, enrollment must be repeated at regular intervals.

Once subjects are enrolled, the amount of time the system requires to scan and process them is the throughput rate. The more complex or detailed the biometric characteristic, the longer the processing will take. Subjects typically accept a throughput rate of about six seconds or faster.

A subject’s acceptance of a security mechanism is dependent upon many subjective perceptions, including privacy, invasiveness, and psychological and physical discomfort. Subjects may be concerned about transfer of body fluids or revelations of health issues via the biometric scanning devices.

Appropriate Biometric Usage

When selecting a biometric solution for a specific environment, numerous aspects must be considered. These aspects include which type of biometric factor is most suitable for your environment as well as the effectiveness and acceptability of the biometric factor. When comparing different types of biometric factors, often a Zephyr chart is used. A Zephyr chart rates various aspects, functions, or features of different biometrics together on a single easy-to-read diagram (see Figure 1.2).
The effectiveness of biometrics is dependent on how accurate one type of biometric factor is in comparison to others. Here is a commonly accepted order of effectiveness from most to least:

- Palm scan
- Hand geometry
- Iris scan
- Retina pattern
- Fingerprint
- Voice verification
- Facial recognition
- Signature dynamics
- Keystroke dynamics
The acceptance of biometrics is a rating of how well people accept the use of specific biometric factors in their environment. The rating of acceptance incorporates a person’s view of how invasive and easy to use a specific type of biometric factor is and the level of health risk it presents. Here is a commonly accepted order of acceptance level from most to least:

- Iris scan
- Keystroke dynamics
- Signature dynamics
- Voice verification
- Facial recognition
- Fingerprint
- Palm scan
- Hand geometry
- Retina pattern

**Tokens**

Tokens are password-generating devices that subjects must carry with them. Token devices are a form of “something you have.” A token can be a static password device, such as an ATM card. To use an ATM card, you must supply the token (the ATM card itself) and your PIN. Tokens can also be one-time or dynamic password devices that look a bit like small calculators. The device displays a string of characters (a password) for you to enter into the system.

There are four types of token devices:

- Static tokens
- Synchronous dynamic password tokens
- Asynchronous dynamic password tokens
- Challenge-response tokens

A static token can be a swipe card, a smart card, a floppy disk, a USB RAM dongle, or even something as simple as a key to operate a physical lock. Static tokens offer a physical means to provide identity. Static tokens still require an additional factor to provide authentication, such as a password or biometric factor. Most device static tokens host a cryptographic key, such as a private key, digital signature, or encrypted logon credentials. The cryptographic key can be used as an identifier or as an authentication mechanism. The cryptographic key is much stronger than a password because it is pre-encrypted using a strong encryption protocol, it is significantly longer, and it resides only in the token. Static tokens are most often used as identification devices rather than as authentication factors.

A synchronous dynamic password token generates passwords at fixed time intervals. Time interval tokens require that the clock on the authentication server and the clock on the token device be synchronized. The generated password is entered into the system by the subject along with a PIN, pass phrase, or password. The generated password provides the identification, and the PIN/password provides the authentication.
An asynchronous dynamic password token generates passwords based on the occurrence of an event. An event token requires that the subject press a key on the token and on the authentication server. This action advances to the next password value. The generated password and the subject’s PIN, pass phrase, or password are entered into the system for authentication.

Challenge-response tokens generate passwords or responses based on instructions from the authentication system. The authentication system displays a challenge, usually in the form of a code or pass phrase. This challenge is entered into the token device. The token generates a response based on the challenge, and then the response is entered into the system for authentication.

Using token authentication systems is a much stronger security measure than using password authentication alone. Token systems use two or more factors to establish identity and provide authentication. In addition to knowing the username, password, PIN, code, and so on, the subject must be in physical possession of the token device.

However, token systems do have failings. If the battery dies or the device is broken, the subject is unable to gain access. Token devices can be lost or stolen. Tokens should be stored and managed intelligently because once a token system is compromised, it can be difficult and expensive to replace.

Tickets

Ticket authentication is a mechanism that employs a third-party entity to prove identification and provide authentication. The most common and well-known ticket system is Kerberos. Kerberos was developed under Project Athena at MIT. Its name is borrowed from Greek mythology. A three-headed dog named Kerberos guards the gates to the underworld, but in the myth, the three-headed dog faced inward, thus preventing escape rather than preventing entrance.

Single Sign On

Single Sign On (SSO) is a mechanism that allows a subject to be authenticated only once on a system. With SSO, once a subject is authenticated, they can roam the network freely and access resources and services without being rechallenged for authentication. This is considered the primary disadvantage to SSO: Once an account is compromised, the malicious subject has unrestricted access. SSO typically allows for stronger passwords because the subject must memorize only a single password. Furthermore, SSO offers easier administration by reducing the number of locations on which an account must be defined for the subject. SSO can be enabled through authentication systems or through scripts that provide logon credentials automatically when prompted.

Scripts, directory services, thin clients, Kerberos, SESAME, NetSP, scripted access, and KryptoKnight are examples of SSO mechanisms.
Kerberos Functionality

Kerberos is a trusted third-party authentication protocol that can be used to provide a single sign-on solution and to provide protection for logon credentials. Kerberos relies upon symmetric key cryptography, specifically Data Encryption Standard (DES), and provides end-to-end security for authentication traffic between the client and the Key Distribution Center (KDC). Kerberos provides the security services of confidentiality and integrity protection for authentication traffic.

The Kerberos authentication mechanism centers on a trusted server (or servers) that hosts the functions of the KDC, Ticket Granting Service (TGS), and Authentication Service (AS). Generally, the Kerberos central server that hosts all of these services is simply referred to as the KDC. Kerberos uses symmetric key cryptography to authenticate clients to servers. All clients and servers are registered with the KDC, so it maintains the secret keys of all network members.

A complicated exchange of tickets (i.e., cryptographic messages) between clients, network servers, and the KDC is used to prove identity and provide authentication. This allows the client to request resources from the server with full assurance that both the client and the server are who they claim to be. The exchange of encrypted tickets also ensures that no logon credentials, session keys, or authentication messages are ever transmitted in cleartext.

Kerberos tickets have specific lifetimes and use parameters. Once a ticket expires, the client must request a renewal or a new ticket to continue communications with a server.

Limitations of Kerberos

Kerberos is a versatile authentication mechanism that can be used over local LANs, local logons, remote access, and client-server resource requests. However, Kerberos has a single point of failure—the KDC. If the KDC is ever compromised, then the secret key of every system on the network is also compromised. Also, if the KDC goes offline, no subject authentication is possible.

There are other limitations or problems with Kerberos:

- Dictionary and brute force attacks on the initial KDC response to a client may reveal the subject’s password.
- Issued tickets are stored in memory on the client and server.
- Malicious subjects can replay captured tickets if they are reused within their lifetime window.

Access Control Techniques

Once a subject has been identified and authenticated and accountability has been established, they must be authorized to access resources or perform actions. Authorization can occur only after the subject’s identity has been verified through authentication. Systems provide authorization through the use of access controls. Access controls manage the type and extent of access subjects have to objects. There are two primary categories of access control techniques: discretionary and nondiscretionary. Nondiscretionary can be further subdivided into specific techniques, such as mandatory, role-based, and task-based access controls.
A system that employs discretionary access controls allows the owner or creator of an object to control and define subject access to that object. In other words, access control is based on the discretion of the owner. For example, if a user creates a new spreadsheet file, they are the owner of that file. As the owner of the file, they can modify the permissions on that file to grant or deny access to other subjects. Furthermore, access is controlled based on user identity. Discretionary access controls are often implemented using access control lists (ACLs) on objects. Each ACL defines the types of access granted or restricted to individual or grouped subjects. Discretionary access control does not offer a centrally controlled management system because owners can alter the ACLs on their objects. Thus, access is more dynamic than it is with mandatory access controls.

Nondiscretionary access controls are used in a rule-based system in which a set of rules, restrictions, or filters determines what can and cannot occur on the system, such as granting subject access, performing an action on an object, or accessing a resource. Access is not based on administrator or owner discretion and is not focused on user identity. Rather, access is managed by a static set of rules that governs the whole environment.

Mandatory access controls rely upon the use of classification labels. Subjects are labeled by their level of clearance. Objects are labeled by their level of classification or sensitivity. For example, the military uses the labels of top secret, secret, confidential, sensitive but unclassified (SBU), and unclassified. In a mandatory access control system, subjects are able to access objects that have the same or a lower level of classification. An expansion of this access control method is known as need-to-know. Subjects with higher clearance levels are granted access to highly sensitive resources only if their work tasks require such access. If they don’t have a need-to-know, even if they have sufficient clearance, they are denied access.

The use of security labels in mandatory access controls presents some interesting problems. First, for a mandatory access control system to function, every subject and object must have a security label. Depending on the environment, security labels can refer to sensitivity, classification, department, project, and so on. The military security labels mentioned earlier range from highest sensitivity to lowest: top secret, secret, confidential, sensitive but unclassified (SBU), and unclassified. Common corporate or commercial security labels are confidential, proprietary, private, sensitive, and public. Security classifications indicate a hierarchy of sensitivity, but each level is distinct.

Systems that employ role-based or task-based access controls define the ability of a subject to access an object through the use of subject roles (i.e., job descriptions) or tasks (i.e., work functions). If a subject is in a management position, they will have greater access to resources than someone who is in a temporary position. Role-based access controls are useful in environments with frequent personnel changes because access is based on a job description (i.e., a role or task) rather than on a subject’s identity.

Roles and groups serve a similar purpose, but they are different in their deployment and use. They are similar in that they both serve as containers to collect users into manageable units. However, a user can be a member of more than one group. In addition to collecting the rights and permissions from each group, an individual user account may also have rights and permissions assigned directly to it. When roles are used, a user can have only a single role. Users have only the rights and permissions assigned to that role and there are no additional individually assigned rights or permissions.
Some nondiscretionary access controls can be labeled as \textit{lattice-based access controls}. Lattice-based access controls define upper and lower bounds of access for every relationship between a subject and object. These boundaries can be arbitrary, but they usually follow the military or corporate security label levels. A subject with the lattice permissions shown in Figure 1.3 has access to resources up to private and down to sensitive but does not have access to confidential, proprietary, or public resources. Subjects under lattice-based access controls are said to have the least upper bound and the greatest lower bound of access to labeled objects based on their assigned lattice position. One common example of a lattice-based access control is a mandatory access control.

\textbf{FIGURE 1.3} A representation of the boundaries provided by lattice-based access controls

---

**Access Control Methodologies and Implementation**

There are two primary access control methodologies: centralized and decentralized (or distributed). \textit{Centralized access control} implies that all authorization verification is performed by a single entity within a system. \textit{Decentralized access control, or distributed access control}, implies that authorization verification is performed by various entities located throughout a system.

**Centralized and Decentralized Access Control**

Centralized and decentralized access control methodologies offer the benefits and drawbacks that any centralized or decentralized system offers. Centralized access control can be managed by a small team or an individual. Administrative overhead is lower because all changes are made in a single location. A single change affects the entire system. However, centralized access control also has a single point of failure. If system elements are unable to access the centralized access control system, then subject and objects cannot interact. Two examples of centralized access control are Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System (TACACS).
Decentralized access control often requires several teams or multiple individuals. Administrative overhead is higher because the changes must be implemented in numerous locations. Maintaining homogeneity across the system becomes more difficult as the number of access control points increases. Changes made to an individual access control point affect only aspects of the systems that rely upon that specific access control point. Decentralized access control does not have a single point of failure. If an access control point fails, other access control points may be able to balance the load until the control point is repaired, plus objects and subjects that don’t rely upon the failed access control point can continue to interact normally. Domains and trusts are commonly used in decentralized access control systems.

A domain is a realm of trust or a collection of subjects and objects that share a common security policy. Each domain’s access control is maintained independently of that for other domains. This results in decentralized access control when multiple domains are involved. To share resources from one domain to another, a trust is established. A trust is simply a security bridge that is established between two domains and allows users from one domain to access resources in another. Trusts can be one-way only or they can be two-way.

RADIUS and TACACS

Remote Authentication Dial-In User Service (RADIUS) is used to centralize the authentication of remote dial-up connections. A network that employs a RADIUS server is configured so the remote access server passes dial-up user logon credentials to the RADIUS server for authentication. This process is similar to the process used by domain clients sending logon credentials to a domain controller for authentication. Use of an authentication server, such as RADIUS or TACACS, that is separate from the primary remote access server system provides the benefit of keeping auditing and access settings on a system other than the remote access server, thus providing greater security.

RADIUS is defined in RFC 2138. It is primarily used to provide an additional layer of protection against intrusions over dial-up connections. RADIUS supports dynamic passwords and callback security. It acts as a proxy for the remote client because it acts on behalf of the client to obtain authentication on the network. RADIUS acts as a client for the network by requesting authentication in much the same manner as a typical client would. Due to the success of RADIUS, an enhanced version of RADIUS named DIAMETER was developed; it is designed for use on all forms of remote connectivity, not just dial-up.

Terminal Access Controller Access Control System (TACACS) is an alternative to RADIUS. TACACS is available in three versions: original TACACS, XTACACS (Extended TACACS), and TACACS+. TACACS integrates the authentication and authorization processes. XTACACS keeps the authentication, authorization, and accounting processes separate. TACACS+ improves XTACACS by adding two-factor authentication. TACACS and RADIUS operate similarly, and TACACS provides the same functionality as RADIUS. However, RADIUS is based on an Internet standard, whereas TACACS is more of a proprietary (although widely used) solution. TACACS is defined in RFC 1492.
Access Control Administration

Access control administration is the collection of tasks and duties assigned to an administrator to manage user accounts, access, and accountability. A system’s security is based on effective administration of access controls. Remember that access controls rely upon four principles: identification, authentication, authorization, and accountability. In relation to access control administration, these principles transform into three main responsibilities:

- User account management
- Activity tracking
- Access rights and permissions management

Account Administration

User account management involves the creation, maintenance, and closing of user accounts. Although these activities may seem mundane, they are essential to the system’s access control capabilities. Without properly defined and maintained user accounts, a system is unable to establish identity, perform authentication, prove authorization, or track accountability.

Creating New Accounts

The creation of new user accounts is a simple process systematically, but it must be protected or secured through organizational security policy procedures. User accounts should not be created at the whim of an administrator or at the request of anyone. Rather, a stringent procedure should be followed that flows from the HR department’s hiring or promotion procedures.

The HR department should make a formal request for a user account for a new employee. That request should include the classification or security level that should be assigned to the new employee’s user account. The new employee’s department manager and the organization’s security administrator should verify the security assignment. Once the request has been verified, only then should a new user account be created. Creating user accounts outside of established security policies and procedures simply creates holes and oversights that can be exploited by malicious subjects. A similar process for increasing or decreasing an existing user account’s security level should be followed.

As part of the hiring process, new employees should be trained on the security policies and procedures of the organization. Before hiring is complete, employees must sign an agreement committing to uphold the security standards of the organization. Many organizations have opted to craft a document that states that violating the security policy is grounds for dismissal as well as grounds for prosecution under federal, state, and local laws. When passing on the user account ID and temporary password to a new employee, a review of the password policy and acceptable use restrictions should be performed.

The initial creation of a new user account is often called an enrollment. The enrollment process creates the new identity and establishes the factors the system needs to perform authentication. It is critical that the enrollment process be completed fully and accurately. It is also critical that the
identity of the individual being enrolled be proved through whatever means your organization deems necessary and sufficient. Photo ID, birth certificate, background check, credit check, security clearance verification, FBI database search, and even calling references are all valid forms of verifying a person’s identity before enrolling them into your secured system.

Account Maintenance
Throughout the life of a user account, ongoing maintenance is required. Organizations with fairly static organizational hierarchies and low employee turnover or promotion will have significantly less account administration than an organization with a flexible or dynamic organizational hierarchy and high employee turnover and promotion. Most account maintenance deals with altering rights and privileges. Procedures similar to the procedures used when new accounts are created should be established to govern how access is changed throughout the life of a user account. Unauthorized increases or decreases in an account’s access capabilities can result in serious security repercussions.

When an employee is no longer present at an organization, their user account should be disabled, deleted, or revoked. Whenever possible, this task should be automated and tied into the HR department. In most cases, when someone’s paychecks are stopped, that person should no longer have logon capabilities. Temporary or short-term employees should have a specific expiration date programmed into their user account. This maintains a degree of control established at the time of account creation without requiring ongoing administrative oversight.

Account, Log, and Journal Monitoring
Activity auditing, account tracking, and system monitoring are also important aspects of access control management. Without these capabilities, it would not be possible to hold subjects accountable. Through the establishment of identity, authentication, and authorization, tracking the activities of subjects (including how many times they access objects) offers direct and specific accountability. Auditing and monitoring as an aspect of operations security and as an essential element of a secure environment are discussed in Chapter 14, “Auditing and Monitoring.”

Access Rights and Permissions
Assigning access to objects is an important part of implementing an organizational security policy. Not all subjects should be granted access to all objects. Not all subjects should have the same functional capabilities on objects. A few specific subjects should access only some objects; likewise, certain functions should be accessible only by a few specific subjects.

The Principle of Least Privilege
The principle of least privilege arises out of the complex structure that results when subjects are granted access to objects. This principle states that subjects should be granted only the amount of access to objects that is required to accomplish their assigned work tasks. This principle has a converse that should be followed as well: subjects should be blocked from accessing objects that are not required by their work tasks.
A related principle in the realm of mandatory access control environments is known as need-to-know. Within a specific classification level or security domain, some assets or resources may be sectioned off or compartmentalized. Such resources are restricted from general access even to those subjects with otherwise sufficient clearance. These compartmentalized resources require an additional level of formalized access approval before they can be used by subjects. Subjects are granted access when they can justify their work-task-related reason for access or their need to know. Often, the need to know is determined by a domain supervisor and is granted only for a limited period of time.

Determining which subjects have access to which objects is a function of the organizational security policy, the organizational hierarchy of personnel, and the implementation of an access control model. Thus, the criteria for establishing or defining access can be based on identity, roles, classifications, location, time, interfaces, need-to-know, and so on.

**Users, Owners, and Custodians**

When discussing access to objects, three subject labels are used: user, owner, and custodian. A user is any subject who accesses objects on a system to perform some action or accomplish a work task. An owner, or information owner, is the person who has final corporate responsibility for classifying and labeling objects and protecting and storing data. The owner may be liable for negligence if they fail to perform due diligence in establishing and enforcing security policies to protect and sustain sensitive data. A custodian is a subject who has been assigned or delegated the day-to-day responsibility of proper storage and protection of objects.

A user is any end user on the system. The owner is typically the CEO, president, or department head. The custodian is typically the IT staff or the system security administrator.

Separation of duties and responsibilities is a common practice that prevents any single subject from being able to circumvent or disable security mechanisms. When core administration or high-authority responsibilities are divided among several subjects, no one subject has sufficient access to perform significant malicious activities or bypass imposed security controls. Separation of duties creates a checks-and-balances system in which multiple subjects verify the actions of each other and must work in concert to accomplish necessary work tasks. Separation of duties makes the accomplishment of malicious, fraudulent, or otherwise unauthorized activities much more difficult and broadens the scope of detection and reporting. It is easy for an individual to perform an unauthorized act if they think they can get away with it. Once two or more people are involved, the committal of an unauthorized activity requires that each person agree to keep a secret. This typically serves as a significant deterrent rather than as a means to corrupt a group en masse.

**Summary**

The first domain of the CISSP CBK is Access Control Systems and Methodology. Access controls are central to the establishment of a secure system. They rely upon identification, authentication, authorization, and accountability. Access control is the management, administration, and implementation of granting or restricting subject access to objects.
Chapter 1 • Accountability and Access Control

The first step in access control is verifying the identities of subjects on the system, commonly known as authentication. There are a number of methods available to authenticate subjects, including passwords and phrases, biometric scans, tokens, and tickets.

Once a subject is authenticated, their access must be managed (authorization) and their activities logged, so ultimately the person can be held accountable for the user account’s online actions.

There are various models for access control or authorization. These include discretionary and nondiscretionary access controls. There are at least three important subdivisions of nondiscretionary access control: mandatory, role-based, and task-based access control.

Access can be managed for an entire network at once. Such systems are known as Single Sign On solutions. Remote access clients pose unique challenges to LAN security and often require specialized tools such as RADIUS or TACACS.

Finally, once all these systems are in place, they must be maintained. It does very little good to set up system security only to let it go stale over time. Proper role assignment and object maintenance are key aspects to keeping a system secure over time.

Exam Essentials

Understand the CIA Triad. The CIA Triad comprises confidentiality, integrity, and availability. Confidentiality involves making sure that each aspect of a system is properly secured and accessible only by subjects who need it. Integrity assures that system objects are accurate and reliable. Availability ensures that the system is performing optimally and that authenticated subjects can access system objects when they are needed.

Know the common access control techniques. Common access control techniques include discretionary, mandatory, nondiscretionary, rule-based, role-based, and lattice-based. Access controls are used to manage the type and extent of access subjects have to objects, which is an important part of system security because such controls define who has access to what.

Understand access control administration. The secure creation of new user accounts, the ongoing management and maintenance of user accounts, auditing/logging/monitoring subject activity, and assigning and managing subject access are important aspects of keeping a system secure. Security is an ongoing task, and administration is how you keep a system secure over time.

Know details about each of the access control models. There are two primary categories of access control techniques: discretionary and nondiscretionary. Nondiscretionary can be further subdivided into specific techniques, such as mandatory, role-based, and task-based access control.

Understand the processes of identification and common identification factors. The processes of identification include subject identity claims by using a username, user ID, PIN, smart card, biometric factors, and so on. They are important because identification is the first step in authenticating a subject’s identity and proper access rights to objects.

Understand the processes of authentication and the various authentication factors. Authentication involves verifying the authentication factor provided by a subject against the authentication factor stored for the claimed identity, which could include passwords, biometrics, tokens, tickets,
SSO, and so on. In other words, the authentication process ensures that a subject is who they claim to be and grants object rights accordingly.

**Understand the processes of authorization.** Authorization ensures that the requested activity or object access is possible given the rights and privileges assigned to the authenticated identity. This is important because it maintains security by providing proper access rights for subjects.

**Understand the strengths and weaknesses of passwords.** Users typically choosing passwords that are easy to remember and therefore easy to guess or crack is one weakness associated with passwords. Another is that randomly generated passwords are hard to remember, thus many users write them down. Passwords are easily shared and can be stolen through many means. Additionally, passwords are often transmitted in cleartext or with easily broken encryption protocols, and password databases are often stored in publicly accessible online locations. Finally, short passwords can be discovered quickly in brute force attacks. On the other hand, passwords can be effective if selected intelligently and managed properly. It is important to change passwords frequently; the more often the same password is used, the more likely it will be compromised or discovered.

**Know the two access control methodologies and implementation examples.** Access control methodologies include centralized access control, in which authorization verification is performed by a single entity within a system, and decentralized access control, in which authorization verification is performed by various entities located throughout a system. Remote authentication mechanisms such as RADIUS and TACACS are implementation examples; they are used to centralize the authentication of remote dial-up connections.

**Understand the use of biometrics.** Biometric factors are used for identification or authentication. FRR, FAR, and CER are important aspects of biometric devices. Fingerprints, face scans, iris scans, retina scans, palm topography, palm geography, heart/pulse pattern, voice pattern, signature dynamics, and keystroke patterns are commonly used in addition to other authentication factors, such as a password, to provide an additional method to control authentication of subjects.
Review Questions

1. What is access?
   A. Functions of an object
   B. Information flow from objects to subjects
   C. Unrestricted admittance of subjects on a system
   D. Administration of ACLs

2. Which of the following is true?
   A. A subject is always a user account.
   B. The subject is always the entity that provides or hosts the information or data.
   C. The subject is always the entity that receives information about or data from the object.
   D. A single entity can never change roles between subject and object.

3. What are the elements of the CIA Triad?
   A. Confidentiality, integrity, and availability
   B. Confidentiality, interest, and accessibility
   C. Control, integrity, and authentication
   D. Calculations, interpretation, and accountability

4. Which of the following types of access control uses fences, security policies, security awareness training, and antivirus software to stop an unwanted or unauthorized activity from occurring?
   A. Preventative
   B. Detective
   C. Corrective
   D. Authoritative

5. __________ access controls are the hardware or software mechanisms used to manage access to resources and systems and to provide protection for those resources and systems.
   A. Administrative
   B. Logical/technical
   C. Physical
   D. Preventative

6. What is the first step of access control?
   A. Accountability logging
   B. ACL verification
   C. Subject authorization
   D. Subject identification
7. ________________ is the process of verifying or testing the validity of a claimed identity.
   A. Identification
   B. Authentication
   C. Authorization
   D. Accountability

8. Which of the following is an example of a Type 2 authentication factor?
   A. Something you have, such as a smart card, ATM card, token device, and memory card
   B. Something you are, such as fingerprints, voice print, retina pattern, iris pattern, face shape, palm topology, and hand geometry
   C. Something you do, such as type a pass phrase, sign your name, and speak a sentence
   D. Something you know, such as a password, personal identification number (PIN), lock combination, pass phrase, mother’s maiden name, and favorite color

9. Which of the following is not a reason why using passwords alone is a poor security mechanism?
   A. When possible, users choose easy-to-remember passwords, which are therefore easy to guess or crack.
   B. Randomly generated passwords are hard to remember, thus many users write them down.
   C. Short passwords can be discovered quickly in brute force attacks only when used against a stolen password database file.
   D. Passwords can be stolen through many means, including observation, recording and playback, and security database theft.

10. Which of the following is not a valid means to improve the security offered by password authentication?
    A. Enabling account lockout controls
    B. Enforcing a reasonable password policy
    C. Using password verification tools and password cracking tools against your own password database file
    D. Allowing users to reuse the same password

11. What can be used as an authentication factor that is a behavioral or physiological characteristic unique to a subject?
    A. Account ID
    B. Biometric factor
    C. Token
    D. IQ
26   Chapter 1 • Accountability and Access Control

12. What does the Crossover Error Rate (CER) for a biometric device indicate?
   A. The sensitivity is tuned too high.
   B. The sensitivity is tuned too low.
   C. The False Rejection Rate and False Acceptance Rate are equal.
   D. The biometric device is not properly configured.

13. Which if the following is not an example of an SSO mechanism?
   A. Kerberos
   B. KryptoKnight
   C. TACACS
   D. SESAME

14. ______________ access controls rely upon the use of labels.
   A. Discretionary
   B. Role-based
   C. Mandatory
   D. Nondiscretionary

15. A network environment that uses discretionary access controls is vulnerable to which of the following?
   A. SYN flood
   B. Impersonation
   C. Denial of service
   D. Birthday attack

16. What is the most important aspect of a biometric device?
   A. Accuracy
   B. Acceptability
   C. Enrollment time
   D. Invasiveness

17. Which of the following is not an example of a deterrent access control?
   A. Encryption
   B. Auditing
   C. Awareness training
   D. Antivirus software
18. Kerberos provides the security services of ________________ protection for authentication traffic.
   A. Availability and nonrepudiation
   B. Confidentiality and authentication
   C. Confidentiality and integrity
   D. Availability and authorization

19. Which of the following forms of authentication provides the strongest security?
   A. Password and a PIN
   B. One-time password
   C. Pass phrase and a smart card
   D. Fingerprint

20. Which of the following is the least acceptable form of biometric device?
   A. Iris scan
   B. Retina scan
   C. Fingerprint
   D. Facial geometry
Answers to Review Questions

1. B. The transfer of information from an object to a subject is called access.

2. C. The subject is always the entity that receives information about or data from the object. The subject is also the entity that alters information about or data stored within the object. The object is always the entity that provides or hosts the information or data. A subject can be a user, a program, a process, a file, a computer, a database, and so on. The roles of subject and object can switch as two entities, such as a program and a database or a process and a file, communicate to accomplish a task.

3. A. The essential security principles of confidentiality, integrity, and availability are often referred to as the CIA Triad.

4. A. A preventative access control is deployed to stop an unwanted or unauthorized activity from occurring. Examples of preventative access controls include fences, security policies, security awareness training, and antivirus software.

5. B. Logical/technical access controls are the hardware or software mechanisms used to manage access to resources and systems and to provide protection for those resources and systems. Examples of logical or technical access controls include encryption, smart cards, passwords, biometrics, constrained interfaces, access control lists, protocols, firewalls, routers, intrusion detection systems, and clipping levels.

6. D. Access controls govern subjects’ access to objects. The first step in this process is identifying who the subject is. In fact, there are several steps preceding actual object access: identification, authentication, authorization, and accountability.

7. B. The process of verifying or testing the validity of a claimed identity is called authentication.

8. A. A Type 2 authentication factor is something you have. This could include a smart card, ATM card, token device, and memory card.

9. C. Brute force attacks can be used against password database files and system logon prompts.

10. D. Preventing password reuse increases security by preventing the theft of older password database files, which can be used against the current user passwords.

11. B. A biometric factor is a behavioral or physiological characteristic that is unique to a subject, such as fingerprints and face scans.

12. C. The point at which the FRR and FAR are equal is known as the Crossover Error Rate (CER). The CER level is used as a standard assessment point from which to measure the performance of a biometric device.

13. C. Kerberos, SESAME, and KryptoKnight are examples of SSO mechanisms. TACACS is a centralized authentication service used for remote access clients.
14. C. Mandatory access controls rely upon the use of labels. A system that employs discretionary access controls allows the owner or creator of an object to control and define subject access to that object. Nondiscretionary access controls are also called role-based access controls. Systems that employ nondiscretionary access controls define a subject’s ability to access an object through the use of subject roles or tasks.

15. B. A discretionary access control environment controls access based on user identity. If a user account is compromised and another person uses that account, they are impersonating the real owner of the account.

16. A. The most important aspect of a biometric factor is its accuracy. If a biometric factor is not accurate, it may allow unauthorized users into a system.

17. D. Antivirus software is an example of a recovery or corrective access control.

18. C. Kerberos provides the security services of confidentiality and integrity protection for authentication traffic.

19. C. A pass phrase and a smart card provide the strongest authentication security because it is the only selection offering two-factor authentication.

20. B. Of the options listed, retina scan is the least accepted form of biometric device because it requires touching a shared eye cup and can reveal personal health issues.