Information Systems Security

Presented By

Dr. Mohamed Marie

Course Overview

- ✓ 1 Accountability and Access Control
- ✓ 2 Attacks and Monitoring
- ✓ 5 Security Management Concepts and Principles
- ✓ 4 Data and Application Security Issues
- ✓ 5 Malicious Code and Application Attacks

Chapter 1

Accountability and Access Control

This chapter presents the following:

- □Access Control Overview
- □Accountability Overview
- □Access Control Techniques
- □Access Control Models
- □Access Control Administration
- □Identification and Authentication Techniques
- □Access Control Methodologies and Implementation

Access Controls Overview

Access controls ***are security features that control how users and systems communicate and interact with other systems and resources.*** They protect the systems and resources from unauthorized access and can be components that participate in determining the level of authorization after an authentication procedure has successfully completed.

Access ***is the flow of information between a subject and an object***.

A **subject** is an **active entity** ***that requests access to an object or the data within an object***. ***A subject can be a user, program***, or ***process*** that accesses an object to accomplish a task. When a program accesses a file, the program is the subject and the file is the object.

An **object** is a **passive entity** ***that contains information***. An object can be a ***computer, database, file, computer program, directory, or field contained in a table within a database***. ***When you look up information in a database, you are the active subject and the database is the passive object***.

Access Controls Overview

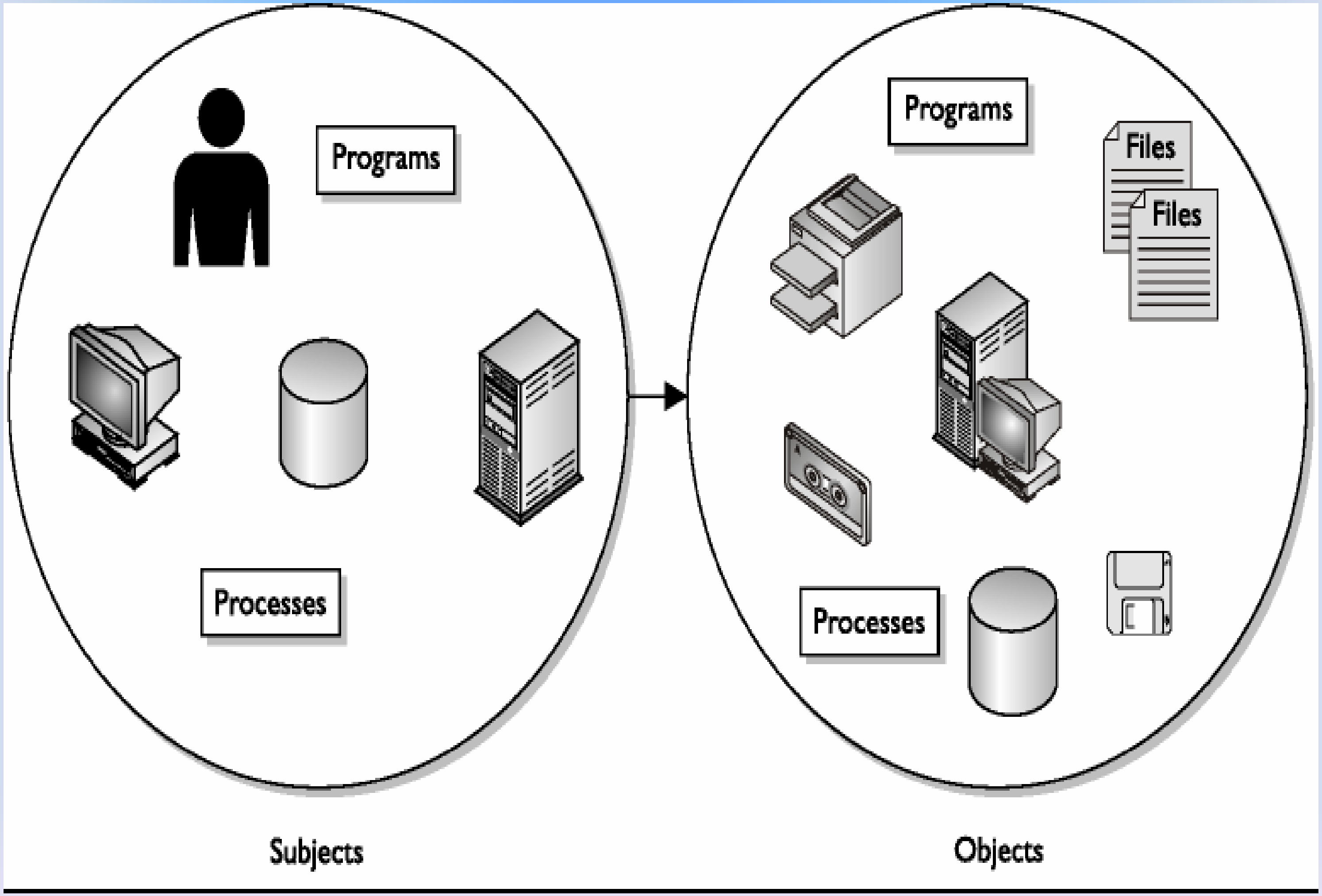


Figure 4-1 Subjects are active entities that access objects, while objects are passive entities.

Access Controls Overview

When a user is prompted for a username and password to use a computer, this is access control.

Once the user logs in and later attempts to access a file, that file may have a list of users and groups that have the right to access it. If the user is not on this list, the user is denied. This is another form of access control. ***The users' permissions and rights may be based on their identity, clearance, and/or group membership.*** Access controls give organizations the ability to ***control***, ***restrict***, ***monitor***, and ***protect*** resource ***availability***, ***integrity***, and ***confidentiality***.

Access Controls Overview

Security Principles

The three main **security principles** for any type of security control are:

-* *Availability*

-* ***Integrity: no unauthorized write***

-* ***Confidentiality: no unauthorized read***

Every control that is used in computer and information security provides at least one of these security principles. It is critical that security professionals understand all of the possible ways these principles can be provided and circumvented.

Access Controls Overview
Availability

Information, systems, and resources *must be available* to users in a *timely manner* so productivity will not be affected.

Most information must be **accessible and available to users when requested** so they can **carry out tasks and fulfill their responsibilities**. **Accessing information does not seem that important until it is inaccessible.**

Administrators experience this when a file server goes offline or a highly used database is out of service for one reason or another.

Fault tolerance and recovery mechanisms are put into place to ensure the continuity of the ***availability*** of resources. User productivity can be greatly affected if requested data is not readily available.

Access Controls Overview
Availability

Information has ***various attributes***, such as ***accuracy***, ***relevance***, ***timeliness***, and ***privacy***. It may be extremely important for a stockbroker to have information that is ***accurate and timely***, so he can buy and sell stocks at the right times at the right prices.

The stockbroker may not necessarily care about the *privacy* of this information, only that it is readily available. A soft drink company that depends on its soda pop recipe would care about the privacy of this trade secret, and the security mechanisms in place need to ensure this secrecy.

Access Controls Overview

Integrity

Information must be ***accurate***, ***complete***, and ***protected*** from unauthorized modification.

When a security mechanism provides integrity, it protects data, or a resource, from being altered in an unauthorized fashion. If any type of illegitimate modification does occur, the security mechanism must alert the user or administrator in some manner.

Integrity of data is very important. What if a confidential e-mail was sent from the Secretary of State to the President of the United States and was intercepted and altered without a security mechanism in place that disallows this or alerts the President that this message has been altered? Instead of receiving a message reading, “We would love for you and your wife to stop by for drinks tonight,” the message could be altered to say, “We have just bombed Libya.” Big difference.

Access Controls Overview
Confidentiality

Confidentiality is the assurance that information is not disclosed to unauthorized individuals, programs, or processes. Some information is more sensitive than other information and requires a higher level of confidentiality. **Control mechanisms** ***need to be in place to dictate who can access data and what the subject can do with it once they have accessed it. These activities need to be controlled, audited, and monitored.*** Examples of information that could be considered confidential are ***health records***, ***financial account information***, ***criminal records***, ***source code***, trade secrets, and military tactical plans.

Some security mechanisms that would provide confidentiality are ***encryption, logical and physical access controls, transmission protocols, database views,*** **and** ***controlled traffic flow.***

Access Controls Overview

Different security mechanisms can supply different degrees of availability, integrity, and confidentiality. **The *environment*, the *classification of the data* that is to be protected, and the *security goals* must be evaluated to ensure the proper security mechanisms are bought and put into place**. Many corporations have wasted a lot of time and money not following these steps and instead buying the new "gee whiz" product that recently hit the market.

Identification, Authentication, Authorization, and Accountability

:

Identification ***describes a method of ensuring that a subject (user, program, or process) is the entity it claims to be***. Identification can be provided with the use of a **username** or **account number**.

To be properly **authenticated**, ***the subject is usually required to provide a second piece to the credential set***. This piece could be a **password**, **passphrase**, **cryptographic key**, **personal identification number (PIN),** or **token**. These two credential items are compared to information that has been previously stored for this subject. If these credentials match the stored information, the subject is authenticated. But we are not done yet.

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.

Identification, Authentication, Authorization, and Accountability

Type 1: A Type 1 authentication factor is ***something you know*** . It is any string of characters that you have memorized and can reproduce on a keyboard when prompted. Examples include a **password**, **PIN**, **passphrase**, **mother's maiden name**, **favorite color**, and so on.

Type 2: A Type 2 authentication factor is ***something you have***. It is a **physical device** that you possess and must have on your person at the time of authentication. Examples of this factor include a **smart card**, **token device**, **memory card**, **USB drive**, and so on. This can also include your **physical location**, referred to as the **somewhere you are factor**.

Identification, Authentication, Authorization, and Accountability

Type 3 A Type 3 authentication factor is ***something you are***. It is a **body part** or a **physical characteristic of your person**. Examples of this factor include **fingerprints**, **voice prints**, **retina patterns**, **iris patterns**, **face shapes**, **palm topology**, **hand geometry**, and so on. This factor is often labeled as a ***biometric*** , or a ***biometric factor***.

As you can see, a ***Type 3*** factor is slightly ***more secure*** than a ***Type 2*** factor, which is in turn ***more secure*** than a ***Type 1*** factor.

Identification, Authentication, Authorization, and Accountability

In addition to these three commonly recognized factors, there are at least two others. One is **something you do** , such as ***writing a signature***, ***typing a passphrase (keyboard dynamics),*** or ***speaking a phrase***. Something you do is often included in the "something you are," or Type 3, category.

Another factor, mentioned earlier, is ***somewhere you are*** , such as the ***computer terminal*** from which you log in or the ***phone number*** (identified by caller ID) or ***country*** (identified by your IP address) from whence you connect.

Identification, Authentication, Authorization, and Accountability

Multiple-Factor Authentication

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 factors of different types***. However, as a general rule, ***when factors of different types are combined, the resultant authentication is more secure***.

Identification, Authentication, Authorization, and Accountability

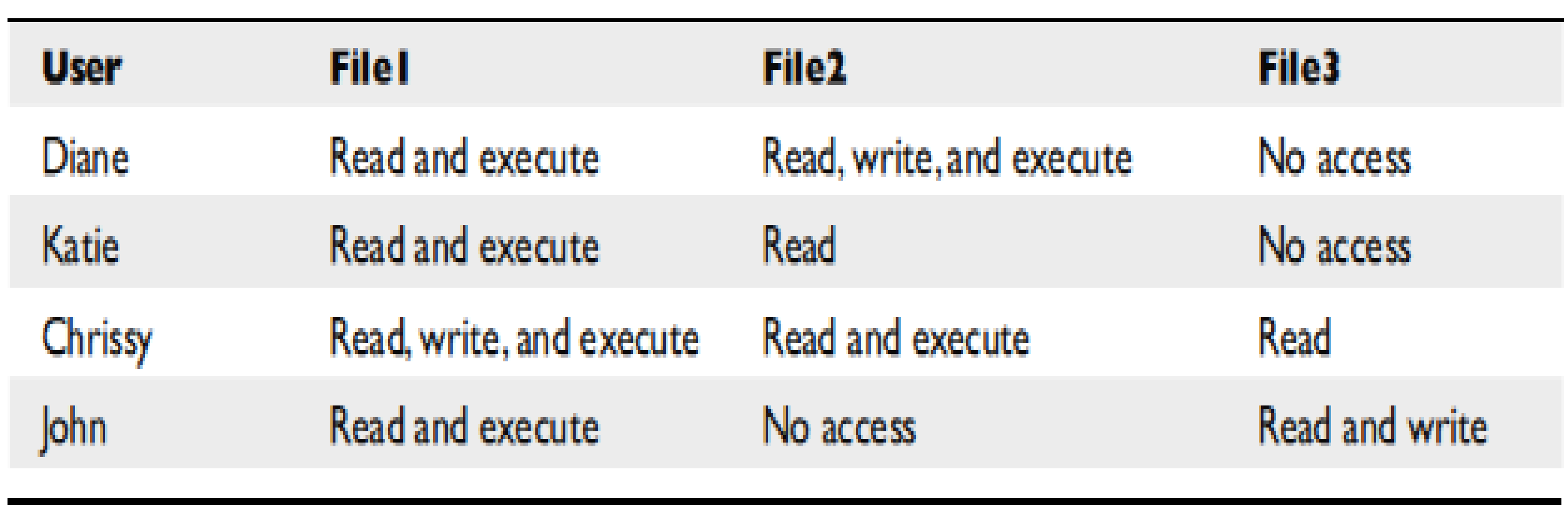
Authorization

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). ***Authorization indicates who is trusted to perform specific operations***. ***In most cases, the system evaluates an*** **access control matrix** ***that compares the subject, the object, and the intended activity***. 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 it has been authorized.

Identification, Authentication, Authorization, and Accountability

Authorization



User	File1	File2	File3
Diane	Read and execute	Read, write, and execute	No access
Katie	Read and execute	Read	No access
Chrissy	Read, write, and execute	Read and execute	Read
John	Read and execute	No access	Read and write

An Example of an Access Control Matrix

Identification, Authentication, Authorization, and Accountability

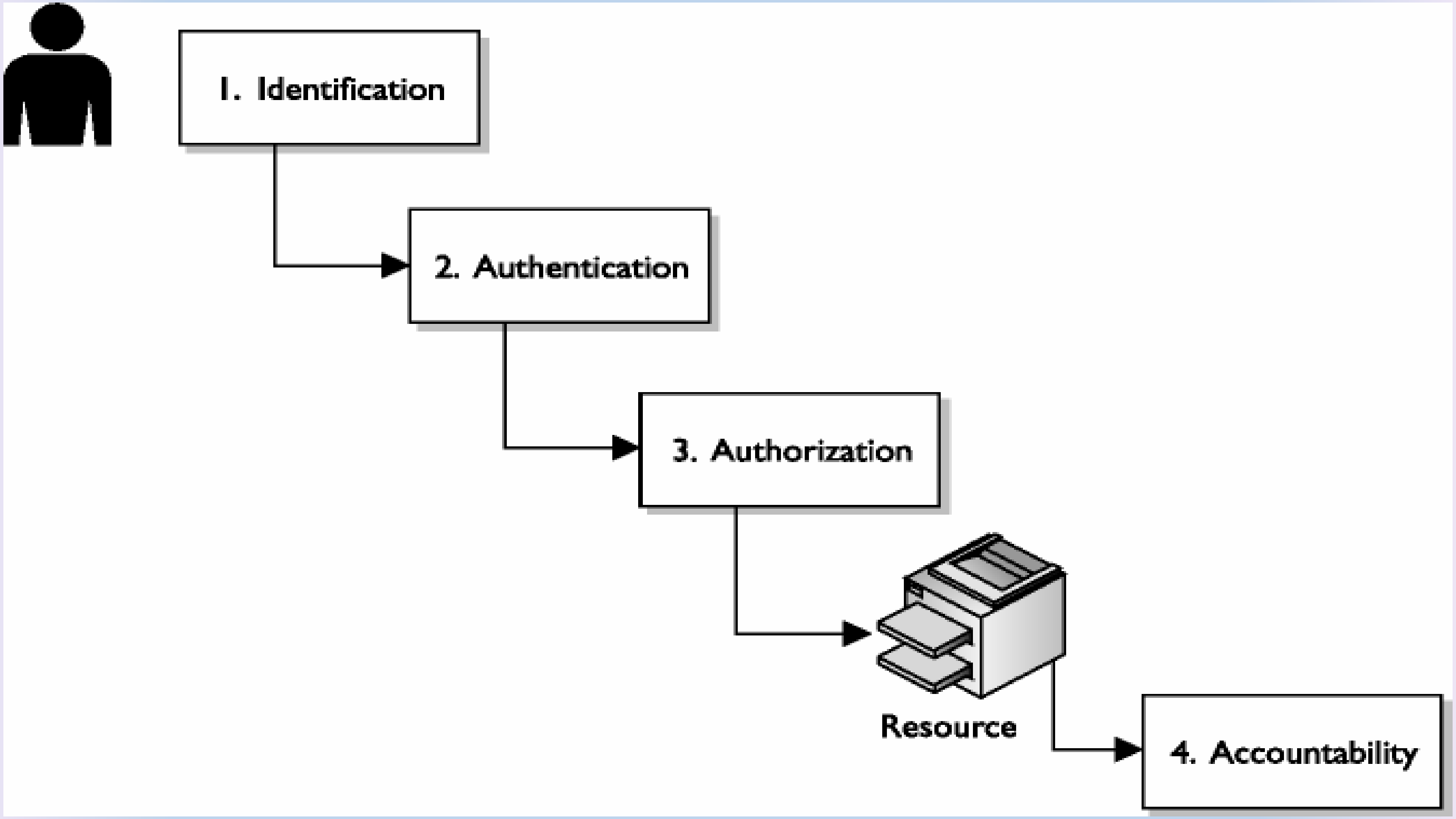


Figure 4-2 Four steps must happen for a subject to access an object: identification, authentication, authorization, and accountability.

Identification, Authentication, Authorization, and Accountability

Auditing and Accountability

Auditing is ***the process by which 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 a security policy or authorization was violated***.

Identification, Authentication, Authorization, and Accountability

Auditing and Accountability

According to the National Institute of Standards and Technology's "**Minimum Security Requirements (MSR)** for Multi-User Operating Systems," document (NISTIR 5153) **audit data recording must comply with the following requirements:**

1- The system shall provide a mechanism for generating a ***security audit trail*** that contains information to support after-the-fact investigation of loss or impropriety and appropriate management response.

2- The system shall provide ***end-to-end user accountability*** for all security-relevant events.

3- The system shall ***protect the security audit trail*** from unauthorized access.

4- The system shall provide a mechanism to ***dynamically control***, during normal system operation, ***the types of events recorded***.

5- The system shall ***protect the audit control mechanisms*** from unauthorized access.

Identification, Authentication, Authorization, and Accountability

Auditing and Accountability

audit data recording must comply with the following requirements:

6- The system shall, by default, ***cause a record to be written to the security audit trail*** for numerous specific security-related events.

7- The system shall provide a ***privileged mechanism to enable or disable the recording of other events into the security audit trail***.

8- For each recorded event, **the audit record shall identify several specific data points at a minimum**.

9- The character strings input as responses to ***password challenges shall not be recorded in the security audit trail***.

10- The audit control mechanism **shall provide an option to enable or disable the recording of invalid user IDs during failed user authentication attempts**.

Identification, Authentication, Authorization, and Accountability

Auditing and Accountability

audit data recording must comply with the following requirements:

11- ***Audit control data*** (for example, audit event masks) ***shall survive system restarts***.

12- The system shall provide a mechanism for ***automatically copying security audit trail files to an alternative storage area*** after a customer-specifiable period of time.

13- The system shall, by default, ***cause a record to be written to the security audit trail*** for numerous specific security-related events.

Identification, Authentication, Authorization, and Accountability

Logical access controls ***are tools used for identification, authentication, authorization, and accountability. They are software components that enforce access control measures for systems, programs, processes, and information.*** The logical access controls can be **embedded** within operating systems, applications, add-on security packages, or database and telecommunication management systems.

Identification Component Requirements

When issuing **identification** values to users, the following should be in place:

1- Each value should be **unique**, for user accountability.

2- A **standard naming scheme** should be followed.

3- The value should be **nondescriptive** of the user's position or tasks.

4- The value should **not be shared** between users.

A subject must provide an **identity** to a system to start the authentication, authorization, and accountability processes. Providing an identity might entail typing 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***.

Identification and Authentication Techniques

Authentication ***verifies the identity of the subject by comparing one or more factors against the database of valid identities (in other words, 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 the first step, and providing the authentication factor(s) is the second step. Without both, a subject cannot gain access to a system—neither element alone is useful.

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:

1- Users typically choose passwords that are ***easy to remember*** and therefore easy to guess or crack.

2- Randomly generated passwords are hard to remember; thus, many users ***write them down***.

3- Passwords are easily ***shared***, ***written down***, and ***forgotten***.

4- Passwords can be ***stolen*** through many means, including observation, recording and playback, and security database theft.

5- Passwords are often ***transmitted in clear text*** or with ***easily broken encryption protocols***.

6- ***Password databases*** are often stored in publicly accessible online locations.

7- ***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 change every time they are used. ***One-time passwords are considered the strongest password type, at least in concept***. Humans can't remember an infinite series of lengthy random character strings, which have only a single-attempt use before expiring. Thus, **one-time passwords are often implemented as Type 2 factors** (***something you have)*** using a processing device known as a **token**.

Password Selection

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, initial passwords for user accounts are ***generated automatically***. 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***. If the algorithm for ***computer-generated passwords is discovered, all passwords created by the system are in jeopardy of being compromised***.

Password Selection

A password mechanism that is slightly more effective than a basic password is a passphrase. A **passphrase** is a ***string of characters usually much longer than a password***. Once the passphrase is entered, the system converts it into a virtual password for use by the authentication process.

Passphrases are often modified ***natural-language sentences*** to simplify memorization. Here's an example: "She ell C shells ByE the c-shor." Using a passphrase has several benefits. It is ***difficult to crack a passphrase*** using a ***brute-force tool***, and the passphrase encourages the use of a password with numerous characters yet is still easy to remember.

Password Selection

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 player in the 1984 World Series?

Password Selection

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** for cognitive password systems is that **each question must be answered at the time of user enrollment (in other words, user account creation) and answered again during the logon process, which increases the time to complete that process**. Cognitive passwords are often employed for phone- or web-based authentication by ***financial organizations***, such as your ***bank***. However, this type of password is considered to be ***inappropriate and insecure*** for protecting IT.

Password Selection

Many systems include password policies that restrict or dictate password characteristics. Common restrictions are requiring a ***minimum length, requiring a minimum age, requiring a maximum age, requiring three or four character types (uppercase, lowercase, numbers, and symbols)***, and **preventing password reuse**.

Password Selection

However, even with **strong software-enforced password restrictions**, **it remains possible to create passwords that may be easily guessed or cracked**. 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 end users create their own passwords, you can offer suggestions like the following for creating strong ones***:

1- **Don't reuse any part of your name**, logon name, email address, employee number, Social Security number, phone number, extension, or other identifying name or code.

2- **Don't use dictionary words**, slang, or industry acronyms.

3- **Do use nonstandard capitalization** and **spelling**.

4- **Do switch letters** and **replace letters with numbers**.

Password Security

When a **malicious user or attacker** seeks to obtain passwords, they can employ several methods, 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 a 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.

Password Security

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***.

Finally, **a hybrid attack** ***attempts a dictionary attack and then performs a type of brute-force attack***. **The follow-up brute- force attack** ***is used to add prefix or suffix characters to passwords from the dictionary to discover one-upped-constructed passwords, two-upped-constructed passwords, and so on.*** A ***one-upped-constructed*** password is a password where a **single character** differs from its form in the dictionary. For example, “password1” is one-upped from “password,” and so are “Password,” “1password,” and “passXword.”

Password Security

No matter what type of password attack is used, only read access is required to the password database. Write access is not required. Therefore, a wider number of user accounts can be employed to launch password-cracking attacks. From an intruder's perspective, this makes finding a weak user account more attractive than having to attack the administrator or root account directly and initially to gain system access.

A social-engineering attack ***is an attempt by an attacker to obtain logon capabilities by deceiving a user, usually over the telephone, into performing specific actions on the system***, such as changing the password of an executive who is on the road or creating a user account for a new fictitious employee.

Password Security

You can improve the security of passwords in several ways. ***Account lockout is a mechanism used to disable a user account after a specified number of failed logons***.

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 (in other words, the computer name or IP address) of the last successful or failed logon attempt appears. 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**.

Password Security

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

1- Use the strongest form of one-way encryption available for password storage.

Never allow passwords to be transmitted over the network in clear text or with weak encryption.

2- ***Use password verification tools*** and ***password-cracking tools against your own password database file***. Require that weak or discovered passwords be changed.

3- ***Disable user accounts for short periods of inactivity***, such as a week or a month.

4- ***Delete accounts that are no longer used***.

5- Properly ***train users about the necessity of maintaining security and the use of strong passwords***. Offer tips and recommendations on how to create strong passwords, such as the following:

5.1- ***Require that users change passwords consistently***. The more secure or sensitive the environment, the more frequently passwords should be changed.

Password Security

5.2- ***Never display passwords in clear form on any screen or within any form.***

5.3- ***Longer passwords***, such as those with 16 characters or more, are harder for a brute-force password-cracking tool to discover. However, it's ***harder for people to remember longer passwords***, which often leads users to write them down. Your organization should have a standard security awareness rule that no passwords should ever be written down. The only possible exception to that rule is that long, ***complex passwords for the most sensitive accounts, such as administrator or root, can be written down and stored in a vault or safety deposit box***.

Password Security

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

1- ***Create lists of passwords users should avoid***. Easy-to-memorize passwords are often easily discovered by password-cracking tools.

2- ***If the root or administrator password is ever compromised, every password on every account should be changed***. (In a high-security environment, a compromised system can never be fully trusted again. Thus, it may require formatting the drives and rebuilding the entire system from scratch.)

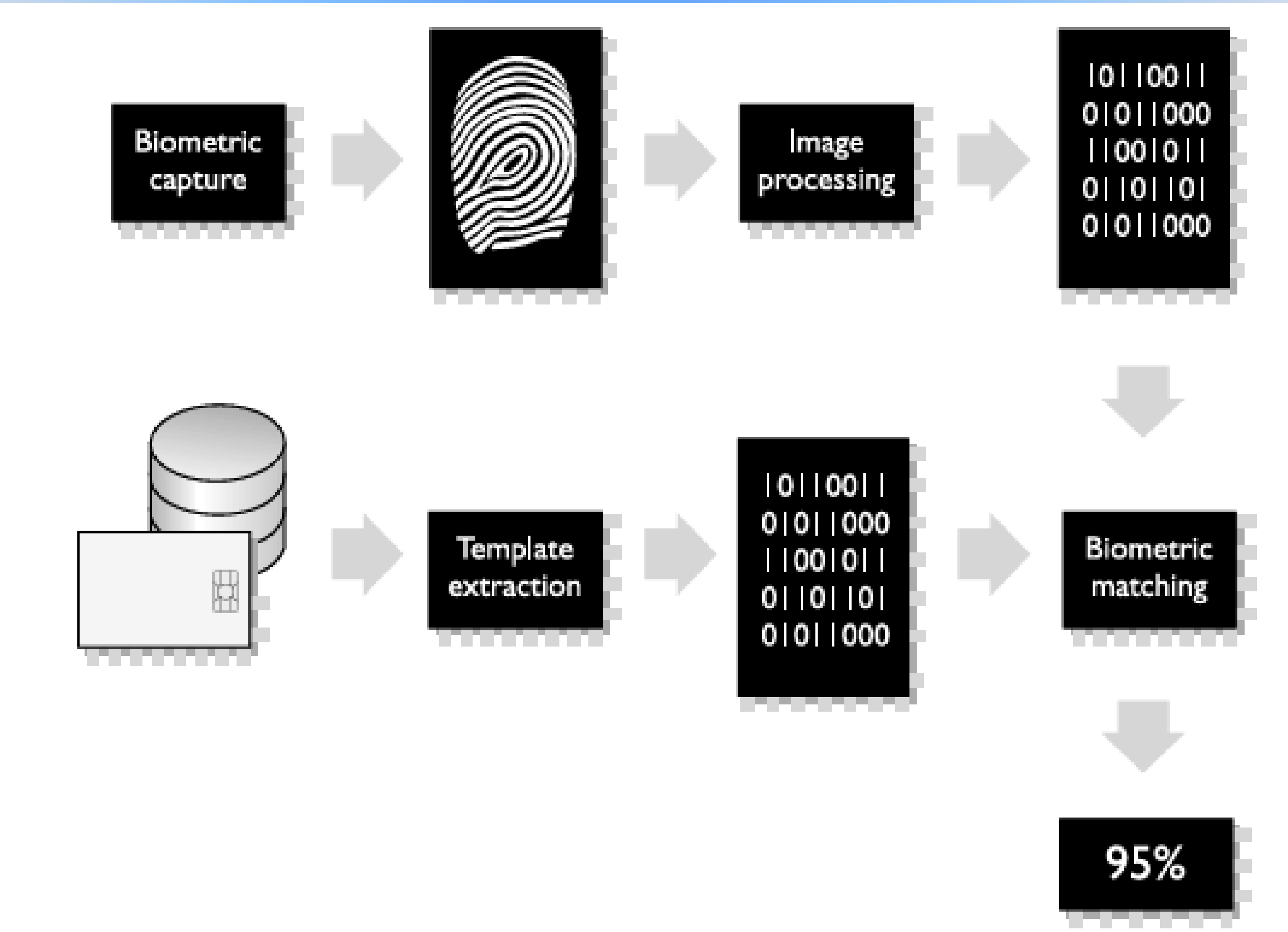
3- ***Never transmit passwords via email***.

Biometrics

Another common authentication and identification technique is the use of ***biometric factors***. Biometric factors fall into the **Type 3**, "***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*), ***hand geometry, heart/pulse patterns, voice patterns, signature dynamics, and keystroke patterns*** (keystroke dynamics).

Biometrics

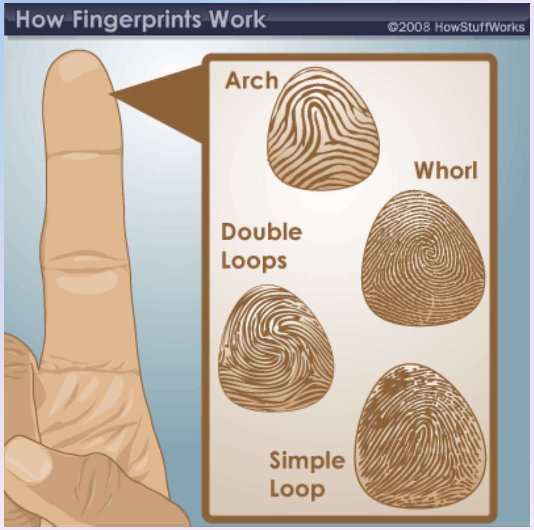


Biometric data is turned into binary data and compared for identity validation.

Biometrics

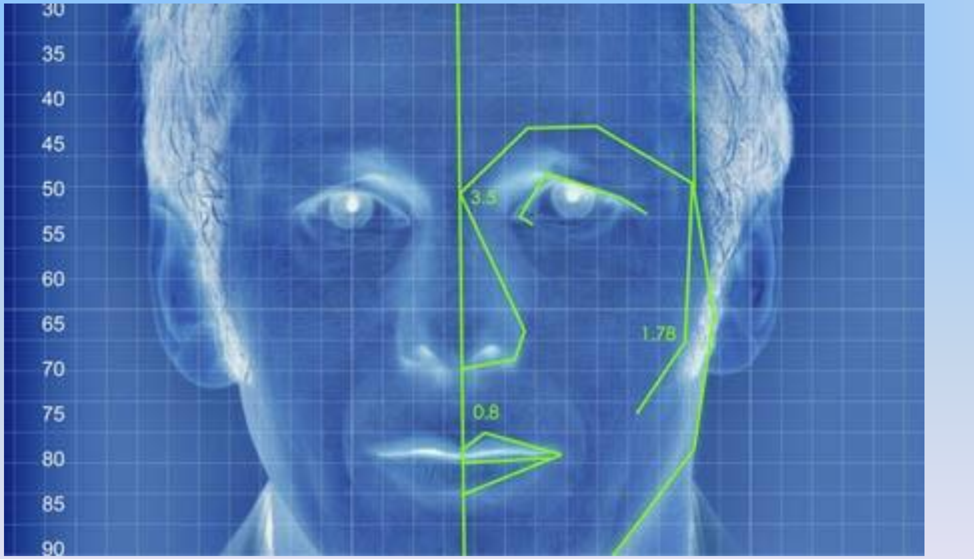
We'll now discuss these biometric factors in more detail, taking into account the human body part they utilize and the information that each quantifies in order to make the most accurate identification possible:

Fingerprints The ***macroscopic*** (in other words, visible to the naked eye) patterns on the last digit of fingers and thumbs are what make fingerprinting so effective for security. A type of fingerprinting known as ***minutia matching*** examines the microscopic view of the fingertips. Unfortunately, minutia matching is affected by small changes to the finger, including ***temperature***, ***pressure***, and ***minor surface damage*** (such as sliding your fingers across a rough surface).



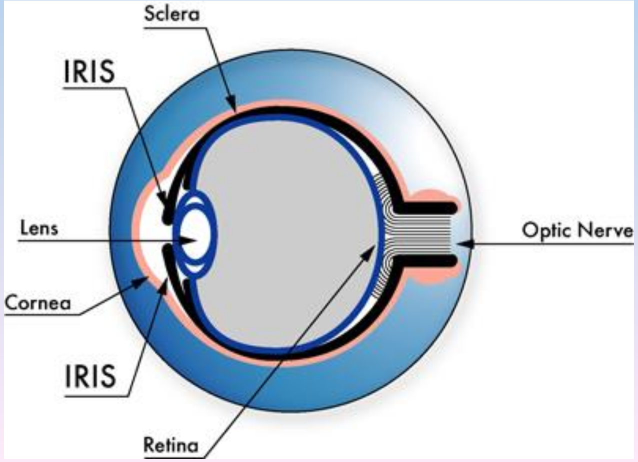
Biometrics

Face scans Face scans utilize the geometric patterns of faces for detection and recognition. They employ the recognition technology known as ***eigenfeatures*** **(facial metrics)** or ***eigenfaces***. (The German word *eigen* refers to recursive mathematics used to analyze intrinsic or unique numerical characteristics.)



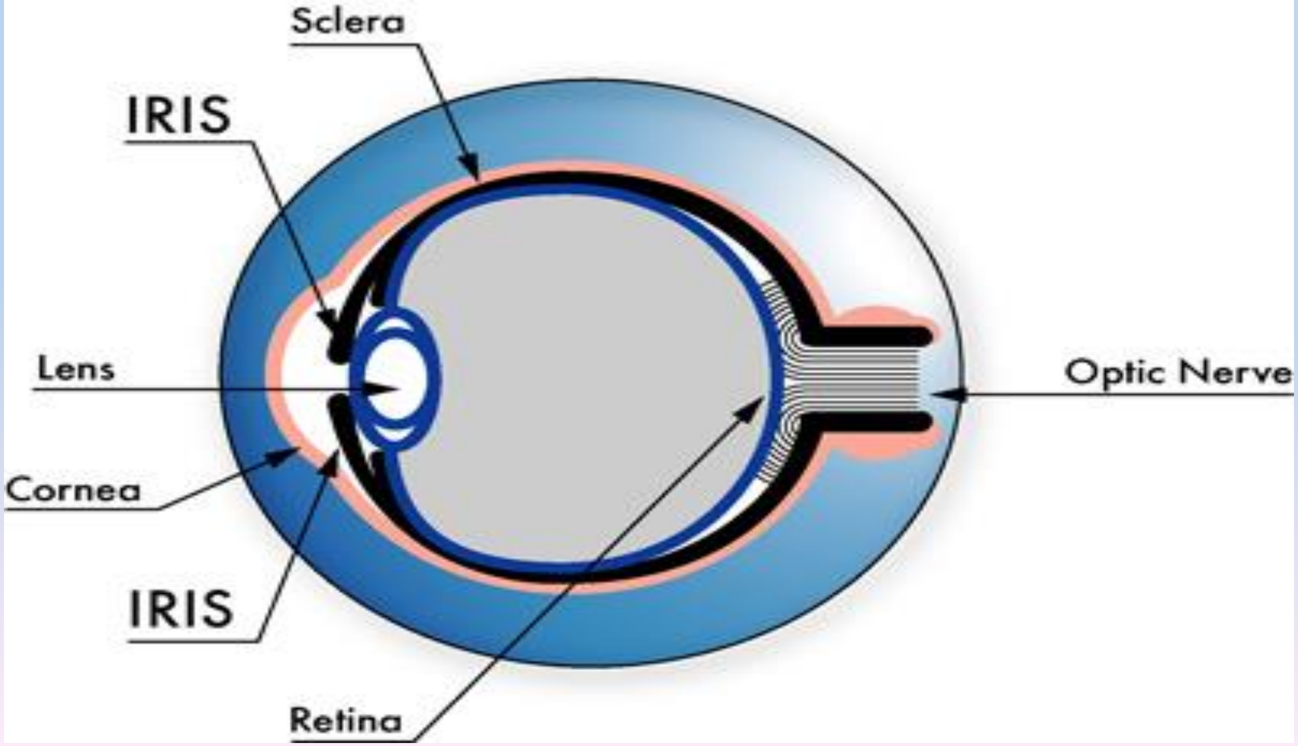
Biometrics

Iris scans ***Focusing on the colored area around the pupil, iris scans are the second most accurate form of biometric authentication***. However, iris scans ***cannot differentiate between identical twins***. Iris scans are often recognized as having a ***longer useful authentication life span than any other biometric factor***. This is because the ***iris remains relatively unchanged throughout a person's life*** (barring eye damage or illness). ***Every other type of biometric factor is more vulnerable and more likely to change over time***. Iris scans are considered acceptable by general users because they don't involve direct contact with the reader and don't reveal personal medical information.



Biometrics

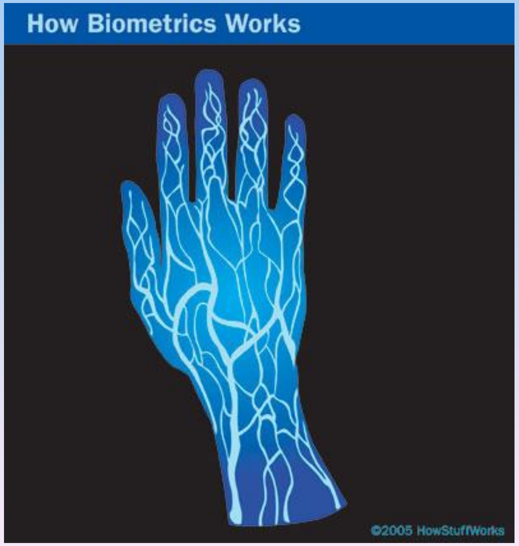
Retina scans Retina scans focus on the pattern of ***blood vessels at the back of the eye. They are the <u>most accurate</u> form of biometric authentication (and are <u>able to differentiate between identical twins</u>) but also <u>the least acceptable</u> because retina scans can reveal medical conditions, such as high blood pressure and pregnancy***. In addition, these types of scans often require a subject to place their eye onto a cup reader that blows air into the eye.



Biometrics

Palm scans Also known as ***palm topography*** or ***palm geography***, ***palm scans utilize the whole area of the hand, including the palm and fingers.*** Palm scans function as a hand-sized fingerprint by analyzing the grooves, ridges, and creases as well as the fingerprints themselves.

Hand geometry Hand geometry recognizes the ***physical dimensions of the hand***. This includes the **width** and **length** of the palm and fingers. This can be a mechanical or image-edge (in other words, visual silhouette) graphical solution.

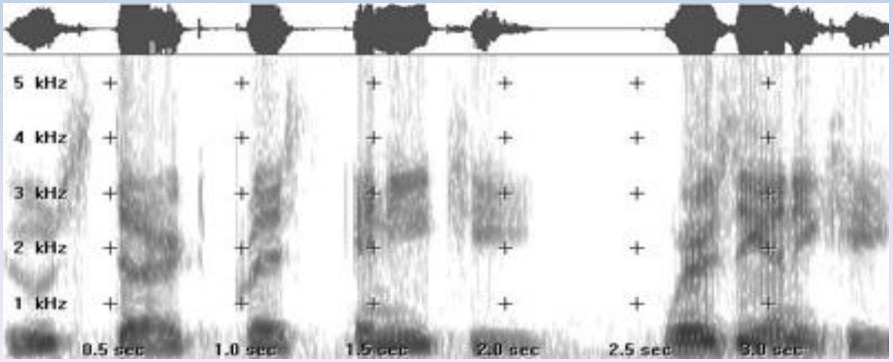


Biometrics

Heart/pulse patterns This involves ***measuring the pulse or heartbeat*** of the user to ensure that a real person is providing the biometric factor. This is often employed as a ***secondary biometric to support one of the other types***.

Biometrics

Voice pattern recognition This type of biometric authentication relies on the ***sound of a subject’s speaking voice***. ***This is different from speech recognition***, which extracts communications from sound (in other words, automatic dictation software). Specifically, ***voice pattern recognition differentiates between one person’s voice and another, while speech recognition differentiates between words within any person’s voice.***



Biometrics

Signature dynamics This recognizes ***how a subject writes a string of characters***. Signature dynamics examine how the subject performs the act of writing as well as features in a written sample. The success of signature dynamics relies upon pen pressure, stroke pattern, stroke length, and the points in time when the pen is lifted from the paper. However, the speed at which the written sample is created is usually not an important factor.

Biometrics

Keystroke patterns (keystroke dynamics) Keystroke patterns measure ***how a subject uses a keyboard by analyzing flight time and dwell time***.

Flight time is ***how long it takes between key presses***, and ***dwell time*** is ***how long a key is pressed***. Using keystroke patterns is **inexpensive**, nonintrusive, and often transparent to the user (both use and enrollment). Unfortunately, using keystroke patterns for security is ***subject to wild variances***. ***Simple changes in user behavior greatly affect this biometric authentication***, such as using only one hand, being cold, standing rather than sitting, changing keyboards, or sustaining an injury to the hand or a finger.

Biometrics

Biometric factors can be used as an identifying or authentication technique. Using a biometric factor instead of a username or account ID as an **identification factor** requires a **one-to-many search** of the offered biometric pattern against the stored database of enrolled and authorized 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.***

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 for identification, a biometric device must be able to detect minute differences in information, such as variations in the blood vessels in a person's retina or 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 performance in producing false negative and false positive authentications. 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 called the **false acceptance rate (FAR).**

Biometric Factor Ratings

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)** or the ***equal error rate*** **(ERR)**; these terms are used interchangeably. The CER level is used as a standard assessment point from which to measure the performance of a biometric device. The **CER or ERR is used** for a single purpose: ***to compare the accuracy of similar biometric devices (in other words, those focusing on the same biometric factor) from different vendors or different models from the same vendor***. On the CER graph, the device with the lowest CER is overall the most accurate.

Biometric Factor Ratings

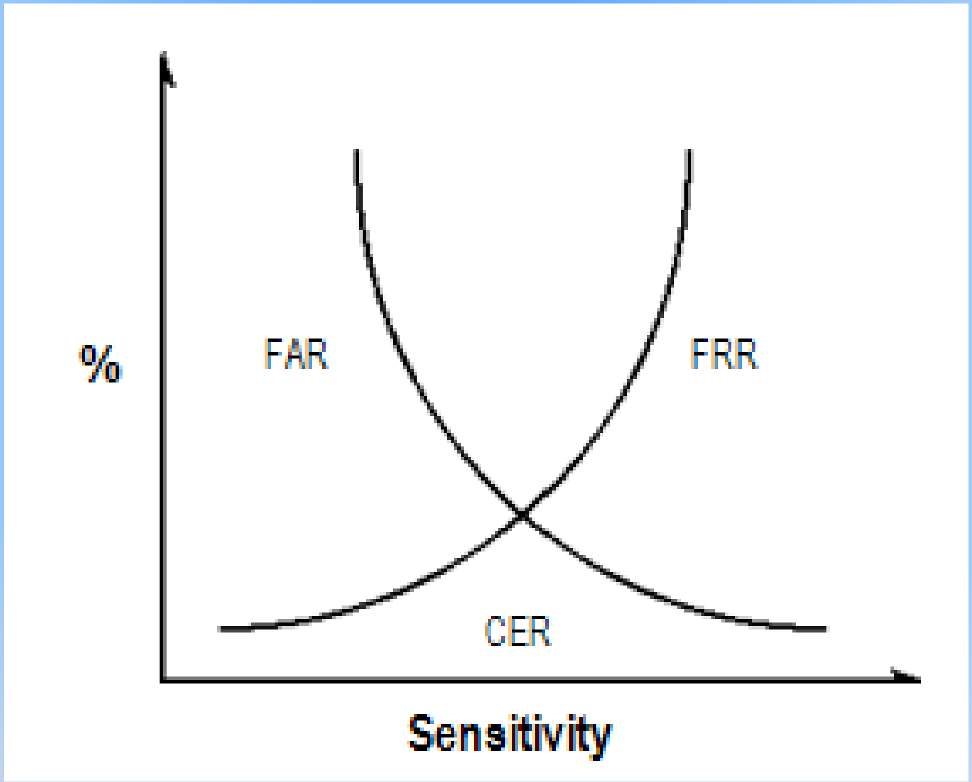


FIGURE 1 . 1 Graph of FRR and FAR errors indicating the CER point

Biometric Registration

In addition to sensitivity issues of biometric devices, several other factors may make them ***less effective***—namely, ***enrollment time***, ***throughput rate***, and ***acceptance***. For a biometric device to work as an identification or authentication mechanism, subjects must be enrolled or registered. This means a subject's biometric factor must be sampled and stored in the device's database. ***The stored sample of a biometric factor is called a*** **reference profile** or a **reference template**. ***The time required to scan and store a biometric factor varies greatly according to which physical or performance characteristic is used.*** The longer it takes to enroll using a biometric mechanism, the less willingly the user community accepts the inconvenience. In general, enrollment times over 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, ***reenrollment*** must occur at regular intervals.

Biometric Registration

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 takes. ***Subjects typically accept a throughput rate of about six seconds or faster***.

A **subject's acceptance** of a security mechanism depends upon many subjective perceptions, including ***privacy***, ***invasiveness***, and ***psychological*** or ***physical discomfort***. Subjects may be concerned about transferring body fluids or may have ***health concerns*** about the biometric-scanning devices.

Appropriate Biometric Usage

When selecting a biometric solution for a specific environment, you must consider numerous aspects. 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, a Zephyr chart is often 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).

Appropriate Biometric Usage

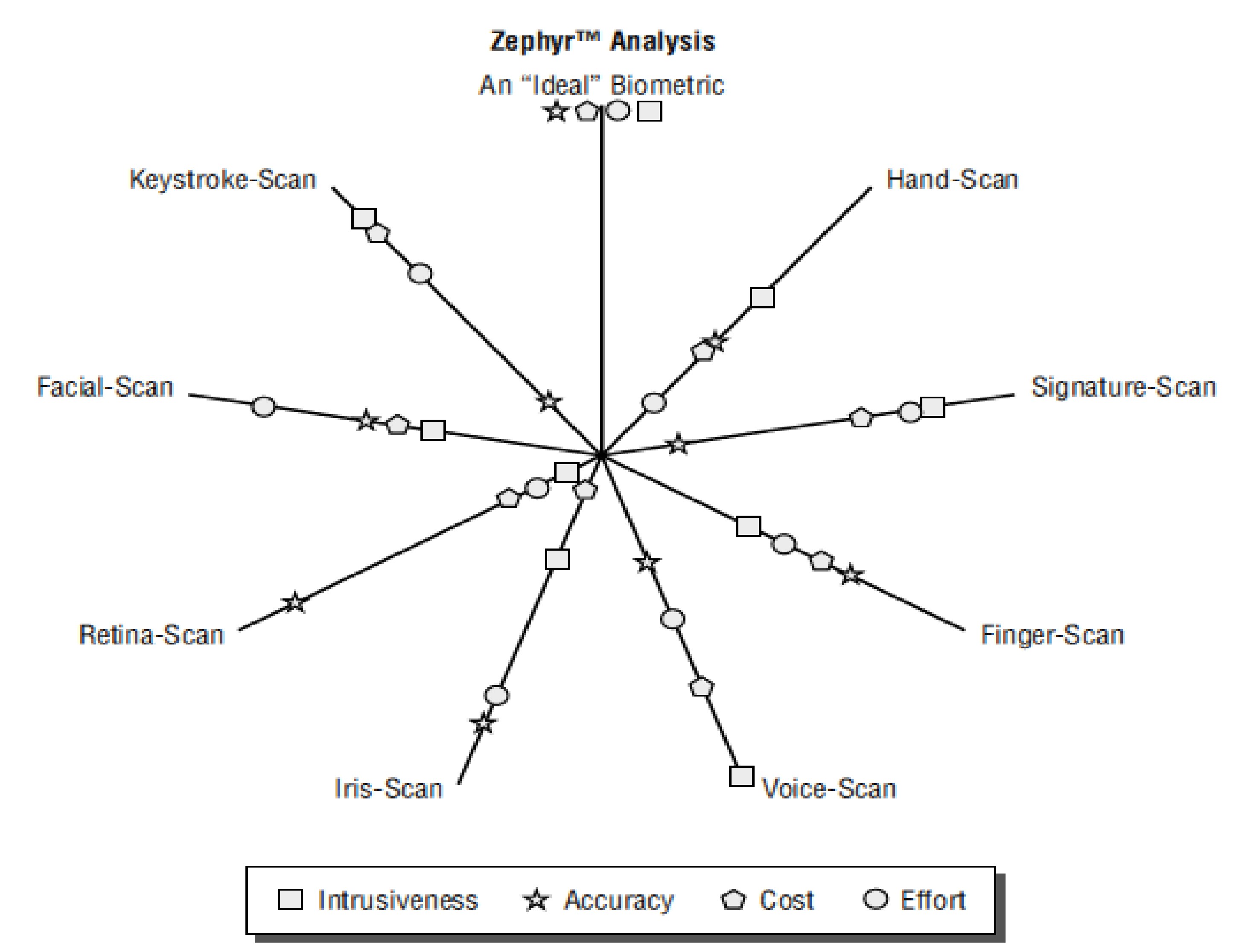


FIGURE 1.2 An example Zephyr chart

Appropriate Biometric Usage

The **effectiveness** of biometrics depends on how accurate one type of biometric factor is in comparison to others. Here is the common order of **accuracy** from most to least:

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

Appropriate Biometric Usage

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 common 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

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***. **A cryptographic key** ***can be used as an identifier or as an authentication mechanism.*** A **cryptographic key** is much stronger than a password because it is preencrypted using strong encryption, 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***.

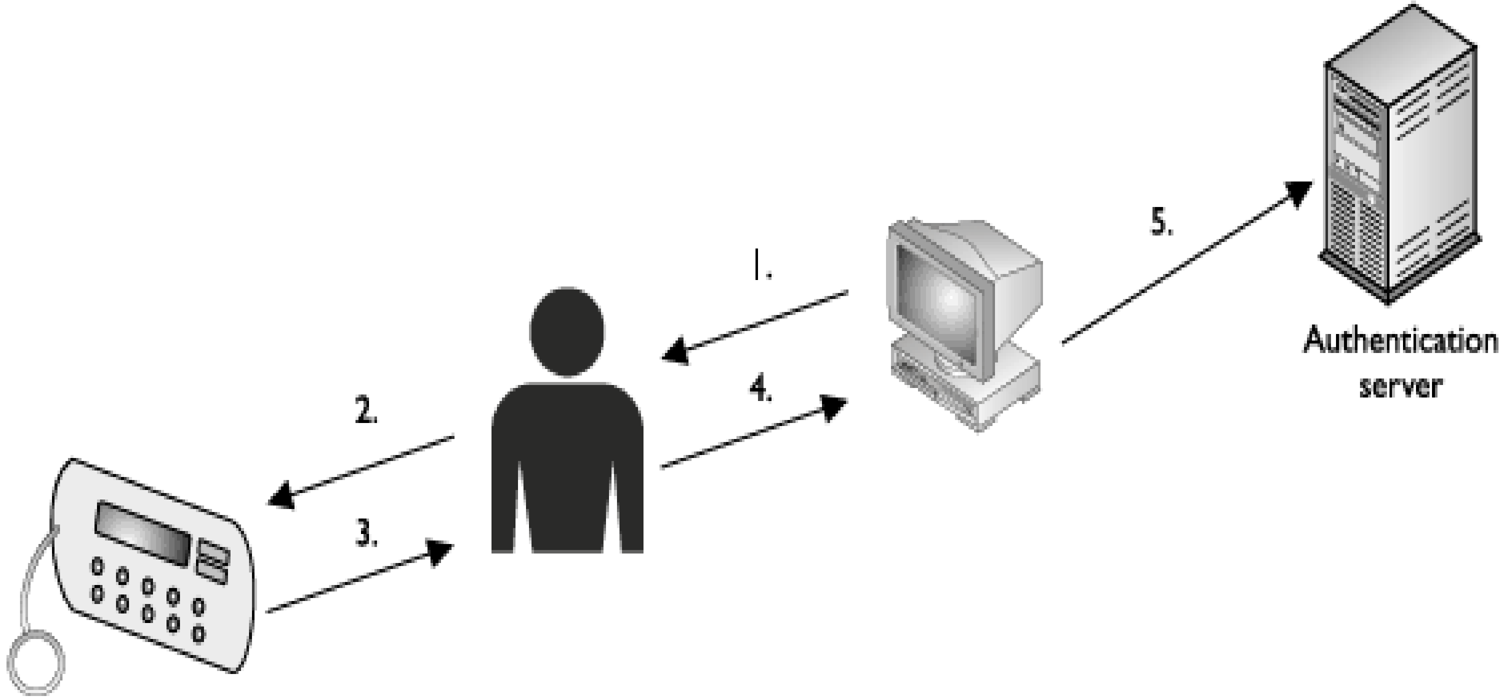
Tokens

A synchronous dynamic password token ***generates passwords at fixed time intervals***. Time interval tokens require synchronizing the clock on the authentication server with the clock on the token device. The subject enters the generated password into the system along with a PIN, passphrase, or password. ***The generated password provides identification, and the PIN/password provides 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, passphrase, 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 passphrase. This challenge is entered into the token device. The token responds to the challenge, and then that response is entered into the system for ***authentication***.

Tokens



1. Challenge value displayed on workstation.
2. User enters challenge value and PIN into token device.
3. Token device presents a different value to the user.
4. User enters new value into the workstation.
5. Value sent to authentication service on server.
6. Authentication service is expecting a specific value.
7. User is authenticated and allowed access to workstation.

Authentication using an <u>asynchronous</u> token device includes a workstation, token device, and authentication service.

Tickets

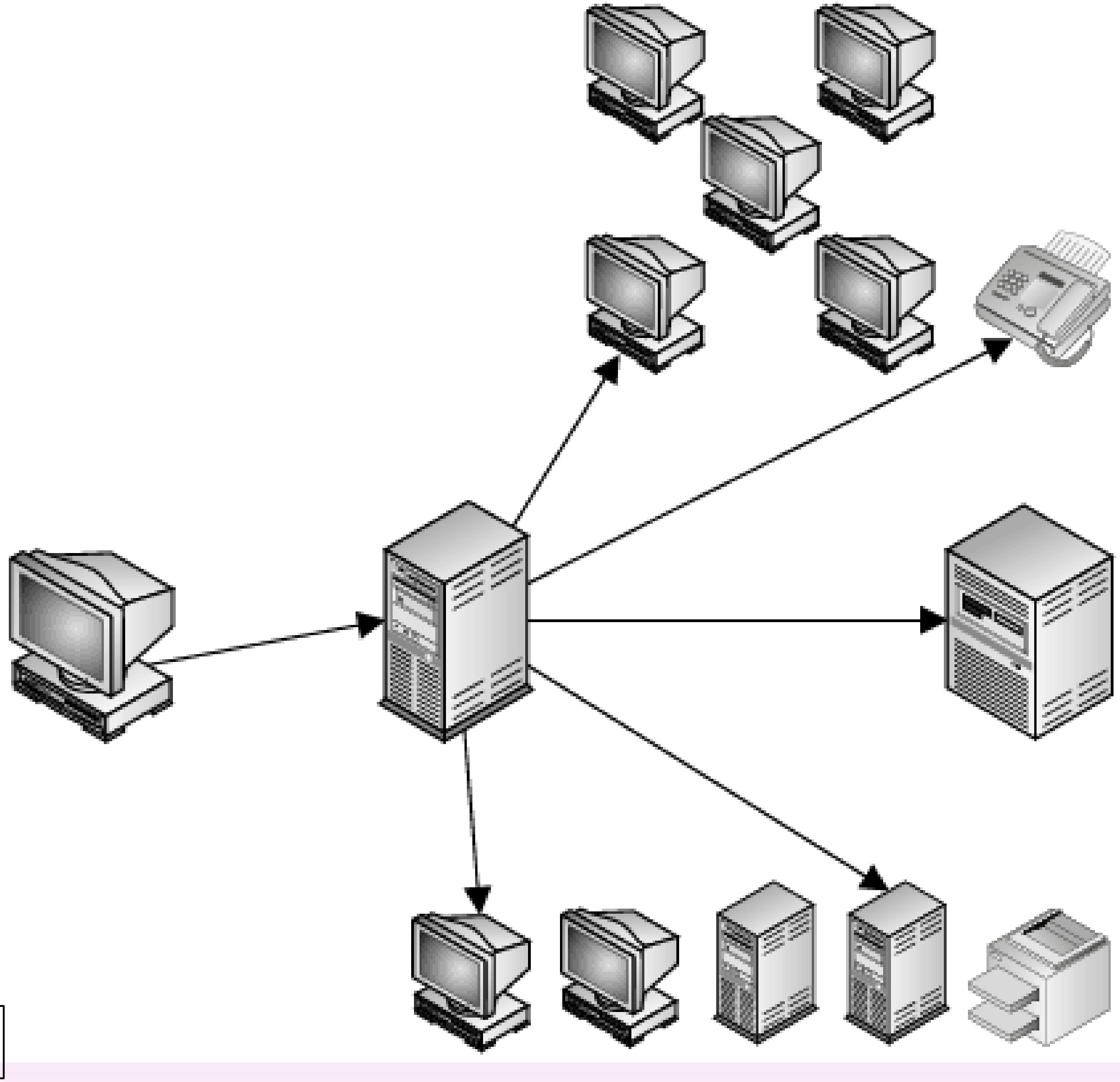
Ticket authentication ***is a mechanism that employs a third-party entity to prove identification and provide authentication*****.** The most common and well-known ticket system is **Kerberos**. Kerberos was developed under Project Athena at MIT. We’ll discuss Kerberos and its tickets later in this chapter.

Single Sign-On

Single sign-on (SSO) ***is a mechanism that allows a subject to be authenticated only once on a system and be able to access resource after resource unhindered by repeated authentication prompts.*** With SSO, once a subject is authenticated, it can roam the network freely and access resources and services ***without further authentication challenges***.

This is considered a **primary disadvantage to SSO**: ***once an account is compromised, a malicious subject has unrestricted access.*** In other words, the maximum level of unauthorized access is gained simply through password disclosure. SSO typically supports stronger passwords because a subject must memorize only a single password. Furthermore, SSO eases administration by reducing the number of locations on which an account must be defined for the subject. You can enable SSO through authentication systems or through scripts that provide logon credentials automatically when prompted.

Single Sign-On



Single sign-on technology enables a user to enter credentials one time to be able to access all preauthorized resources within the domain.

Access Control Techniques

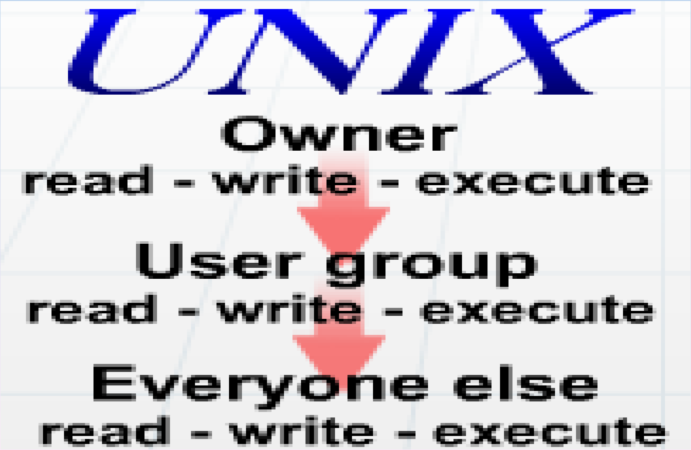
Once a subject has been identified and authenticated and accountability has been established, it must be authorized to access resources or perform actions. Authorization can occur only after the subject's identity has been verified through authentication. Systems provide authorization through the use of access controls. Access controls manage the type and extent of access subjects have to objects. There are two primary categories for access control techniques: ***discretionary and nondiscretionary***. **Nondiscretionary can** be further ***subdivided into specific techniques***, such as ***mandatory, role-based, and task-based access controls***.

There are several forms of access controls that define how subjects access and interact with objects in a variety of ways. Each system has its own security properties that individually distinguish and differentiate it from all others. Each type of system is described in the following sections.

Access Control Techniques

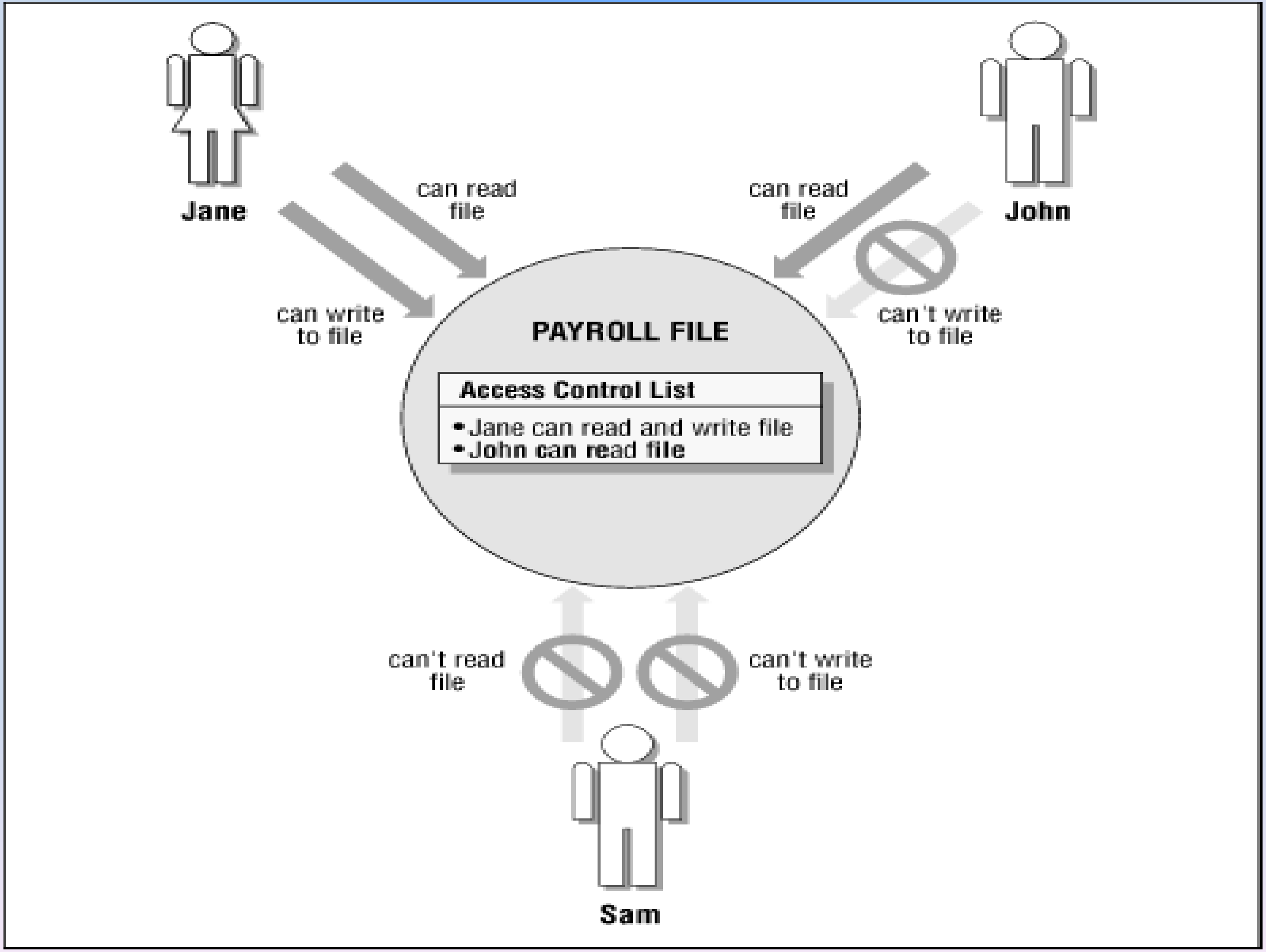
Discretionary Access Controls

A system that employs discretionary access controls (DACs) ***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 (in other words, a decision) of the owner.*** Access is granted or denied in a discretionary environment based on the identity of the subject (which is typically the user account name). For example, if a user creates a new spreadsheet file, that user is the owner of that file. As the owner of the file, that user can modify the permissions on that file to grant or deny access to other subjects. DACs are often implemented using **access control lists** on objects. Each **ACL** ***defines the types of access granted or restricted to individual or grouped subjects.***



Access Control Techniques

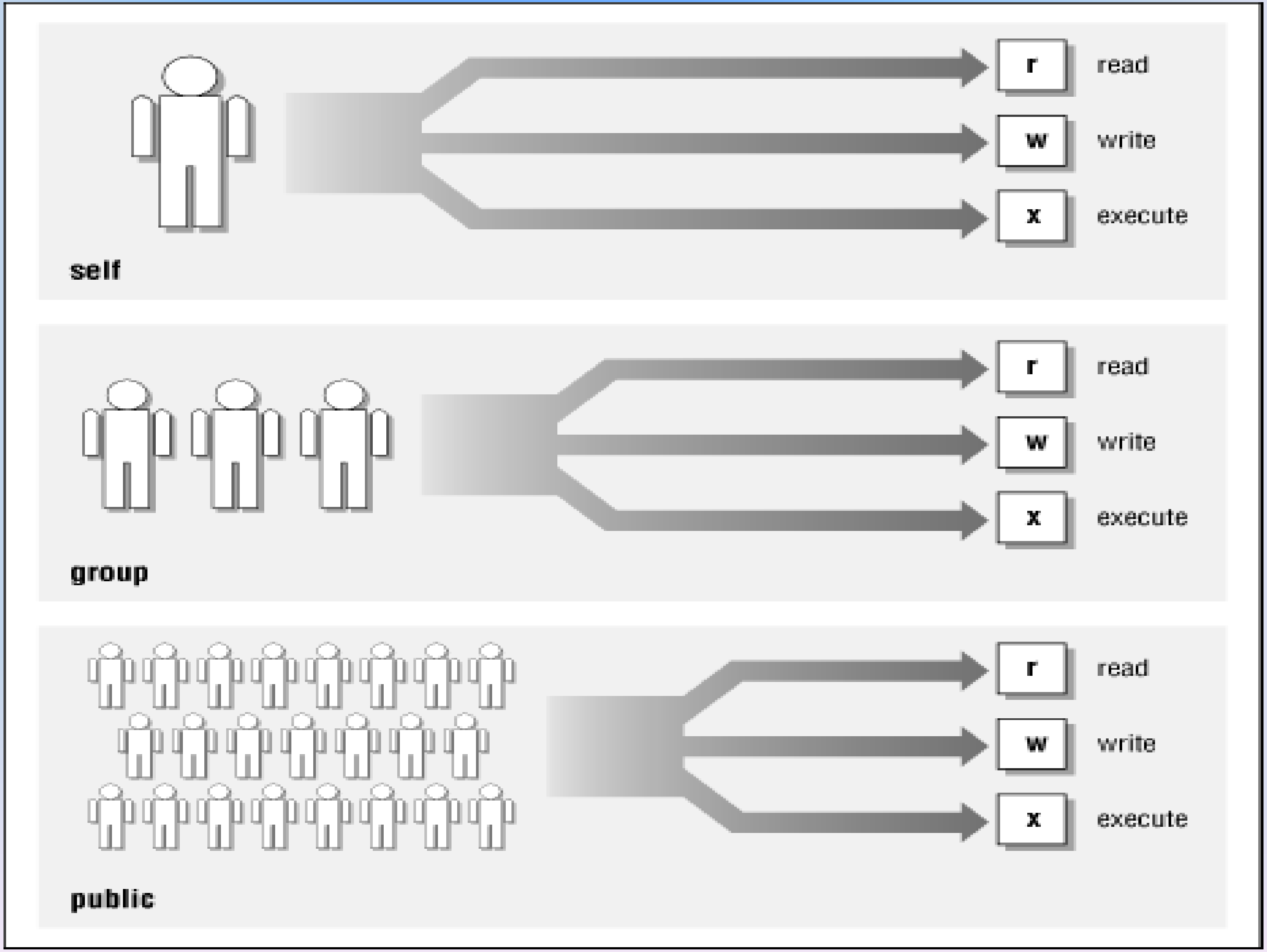
Discretionary Access Controls



Discretionary Access Control With an Access Control List

Access Control Techniques

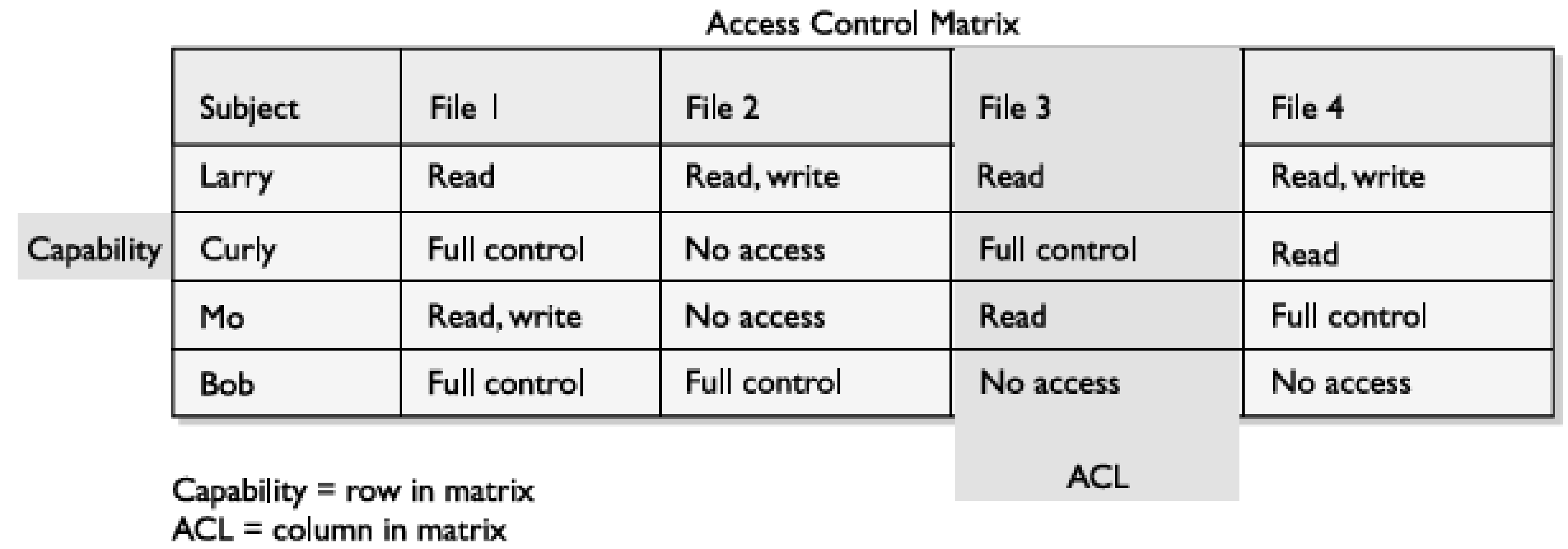
Discretionary Access Controls



Self/Group/Public Controls

Access Control Techniques

Discretionary Access Controls



Access Control Matrix

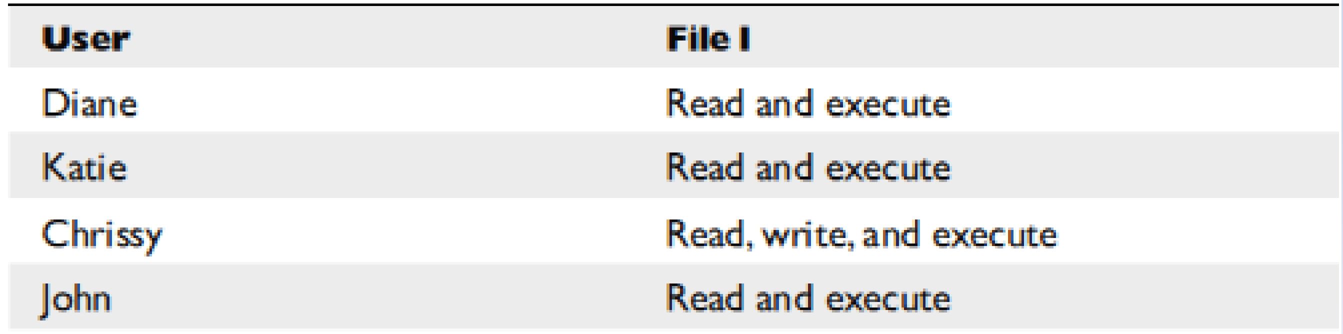
Subject	File 1	File 2	File 3	File 4
Larry	Read	Read, write	Read	Read, write
Curly	Full control	No access	Full control	Read
Mo	Read, write	No access	Read	Full control
Bob	Full control	Full control	No access	No access

Capability

ACL

Capability = row in matrix
ACL = column in matrix

A capability table is bound to a subject, whereas an ACL is bound to an object.



User	File I
Diane	Read and execute
Katie	Read and execute
Chrissy	Read, write, and execute
John	Read and execute

The ACL for File1

Access Control Techniques

Nondiscretionary 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.*** (Thus, nondiscretionary access control is the opposite of discretionary in much the same way as Non-A is the opposite of A.) Rather, ***access is managed by a static set of rules that governs the whole environment*** (in other words, centrally controlled management system).

In general, **rule-based access control systems** ***are more appropriate for environments that experience frequent changes to data permissions*** (in other words, changing the security domain or label of objects). This is ***because rule-based systems can implement sweeping changes just by changing the central rules without having to manipulate or "touch" every subject and/or object in the environment.*** However, in most cases, once the rules are established, they remain fairly static and unchanged throughout the life of the environment.

Access Control Techniques

Nondiscretionary Access Controls

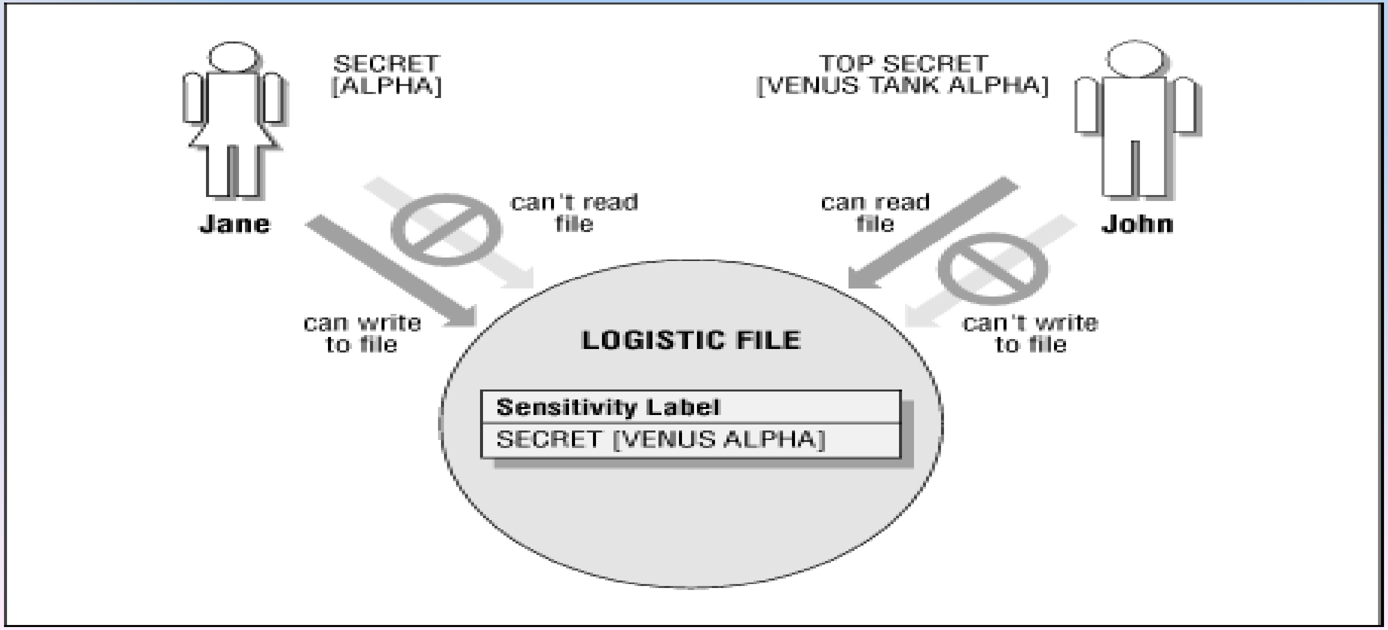
In rule-based access control systems, ***control is based on a specific profile created for each user. A common example of such a system is a firewall.*** **A firewall** ***is governed by a set of rules or filters defined by the administrator.*** Users are able to communicate across the firewall because they have initiated transactions that are allowed by the defined rules. Users are able to accomplish this because they have client environments configured to do so; these are the specific profiles. The formalized definition of a rule-based access control (or specifically, a *rule-based security policy*) is found in RFC 2828, "Internet Security Glossary." This document includes the following **definition for rule-based security policy**: "***A security policy based on global rules imposed for all users***. These rules usually rely on comparison of the sensitivity of the resource being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users."

Access Control Techniques

Nondiscretionary Access Controls

1- Mandatory Access Controls

Mandatory access controls ***rely upon the use of*** ***classification labels*****. *Each classification label represents a security domain or a realm of security. A security domain is a realm of common trust that is governed by a specific security policy for that domain.*** Subjects are labeled by their level of clearance (which is a form of privilege). Objects are labeled by their level of classification or sensitivity. For example, the military uses the labels of **top secret**, **secret**, **confidential**, **sensitive.**



Mandatory Access Control

Access Control Techniques

Nondiscretionary Access Controls

1- Mandatory Access Controls

In a mandatory access control system, subjects are able to access objects that have the same or a lower level of classification.

Subjects with higher clearance levels are granted access to highly sensitive resources only if their work tasks require such access.

MAC is generally recognized as being more secure than DAC but not as flexible or scalable. This relative scale of security is evident via the TCSEC evaluation criteria, which lists mandatory protection as a higher level of security than discretionary protection (for more information about TCSEC, see Chapter 12, “Principles of Security Models”).

Access Control Techniques

Nondiscretionary Access Controls

1- Mandatory Access Controls

Using security labels in mandatory access controls presents some interesting **problems**.

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, value to the organization, need for confidentiality, 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.

Access Control Techniques

Nondiscretionary Access Controls

1- Mandatory Access Controls

Classifications within a mandatory access control environment are of three types:

Hierarchical environments: ***Hierarchical environments relate the various classification labels in an ordered structure from low security to medium security to high security.***

Compartmentalized environments: In compartmentalized environments, ***there is no relationship between one security domain and another***. To gain access to an object, the subject must have the exact specific clearance for that object's security domain.

Access Control Techniques

Nondiscretionary Access Controls

1- Mandatory Access Controls

Classifications within a mandatory access control environment are of three types:

Hybrid environments: ***A hybrid environment combines the hierarchical and compartmentalized concepts so that each hierarchical level may contain numerous subcompartments that are isolated from the rest of the security domain.*** A hybrid MAC environment provides more granular control over access but becomes increasingly difficult to manage as the size of the environment (in other words, number of classifications, objects, and subjects) increases.

Access Control Techniques

Nondiscretionary Access Controls

2- Role-Based Access Control

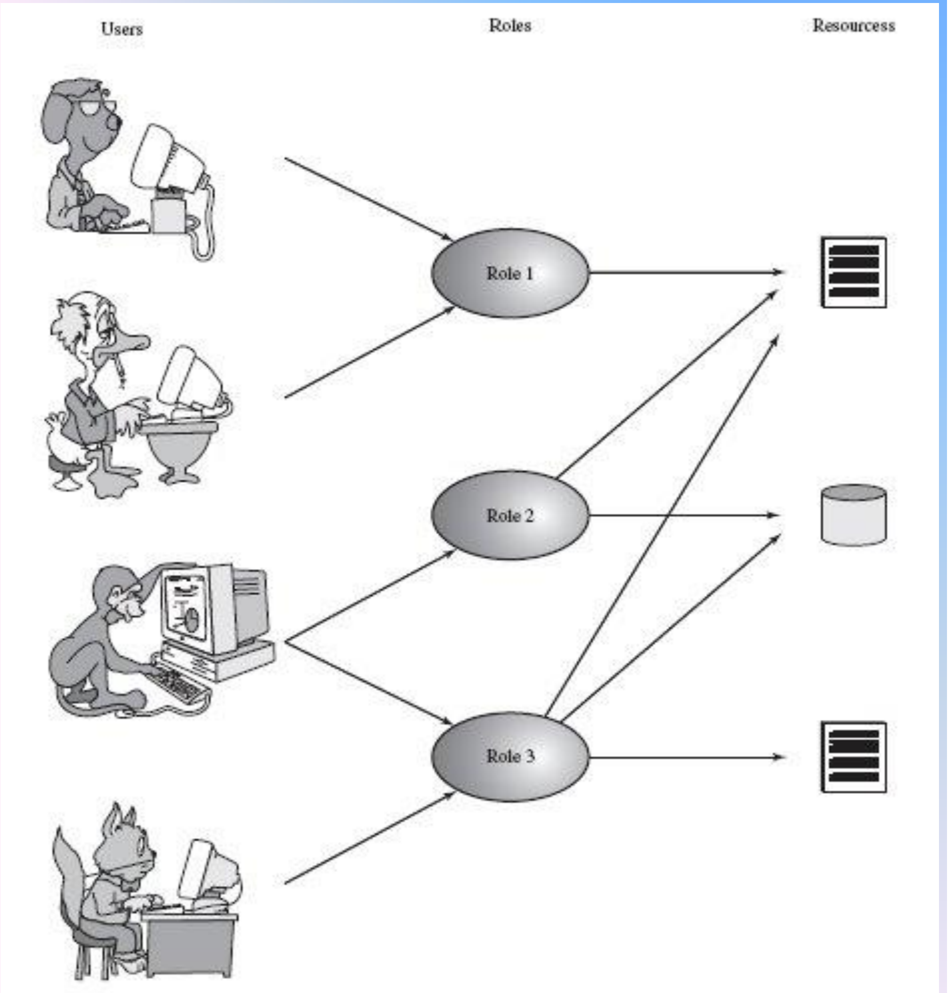
Systems that employ role-based or task-based access controls define a subject's ability to access an object via subject roles (in other words, job descriptions) or tasks (in other words, work functions). If a subject occupies a management position, it will have greater access to resources than a subject who is in a temporary job. Role-based access controls are useful in volatile environments with frequent personnel changes because access depends on a job description (in other words, a role or task) rather than on subject identity.

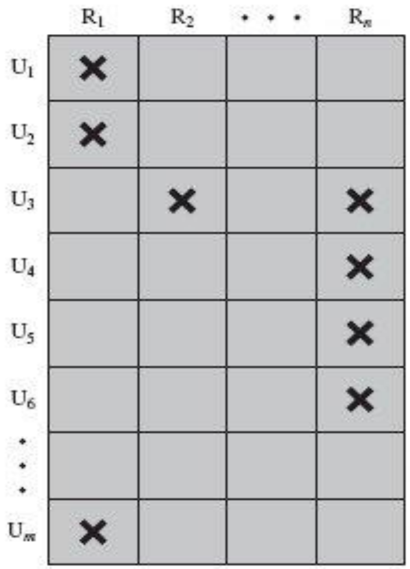
Role-based access control (RBAC) and groups within a DAC environment may serve a similar purpose, but they are different in their deployment and use. They are similar in that both serve as containers to collect users into manageable units. However, a user can belong to more than one group. In addition to collecting rights and permissions from each group, individual user account may also be directly assigned rights and permissions.

Access Control Techniques

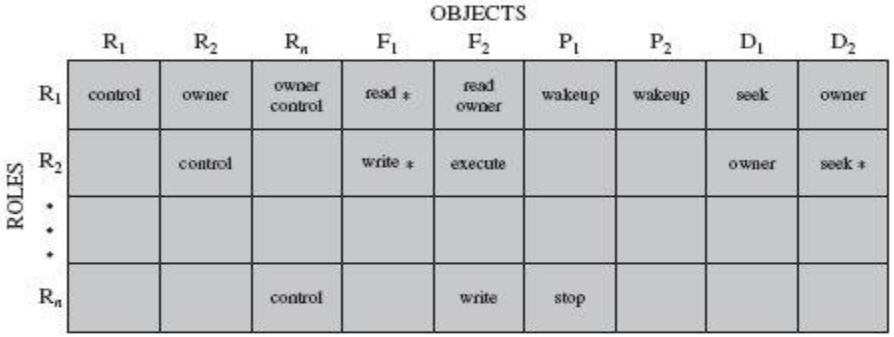
Nondiscretionary Access Controls

2- Role-Based Access Control





	R_1	R_2	• • •	R_n
U_1	✕			
U_2	✕			
U_3		✕		✕
U_4				✕
U_5				✕
U_6				✕
• • •				
U_m	✕			



						OBJECTS				
		R_1	R_2	R_n	F_1	F_2	P_1	P_2	D_1	D_2
ROLES	R_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
	R_2		control		write *	execute			owner	seek *
	• • •									
	R_n			control		write	stop			

Access Control Techniques

Nondiscretionary Access Controls

2- Role-Based Access Control

In a DAC system, even with groups, access is still based on the discretion of an owner and focuses control on the identity of the user. When an RBAC system is employed, a user may have only a single role, but new trends are emerging where a user is assigned multiple roles. Users have only the rights and permissions assigned to such roles, and there are no additional individually assigned rights or permissions. Furthermore, access is not determined by owner discretion; it derives from the inherent responsibilities of the assigned role (in other words, job description). Also, access focuses on the assigned role, not on the identity of the user. Two different users with the same assigned role will have the same access and privileges.

Access Control Techniques

Nondiscretionary Access Controls

2- Role-Based Access Control

RBAC is becoming increasingly attractive to corporate entities that have high rates of employee turnover. This implies that the ***roles or job descriptions within an RBAC system are often _hierarchical_***, meaning that roles are related in a low-to-high fashion so that the higher roles are created by adding access and privileges to lower roles. Often, ***MAC and DAC environments can be replaced by RBAC solutions***.

Another method related to RBAC is called **task-based access control** (TBAC). **TBAC** ***is basically the same as RBAC, but instead of being assigned a single role, each user is assigned dozens of tasks.*** These tasks all relate to assigned work tasks for the person associated with the user account. Under TBAC, access is still based on rules (in other words, on ***work tasks***) and focuses on controlling access by tasks assigned rather than by user identity.

Access Control Techniques

Nondiscretionary Access Controls

3- Lattice-Based Access Controls

Some, if not most, nondiscretionary access controls can be labeled as *lattice-based access controls*. **Lattice-based access controls** ***define upper and lower bounds of access for every relationship between a subject and an object.*** A subject with the lattice permissions shown in Figure 1.3 can access resources up to private and down to sensitive but cannot access confidential, proprietary, or public resources. Subjects under lattice-based access controls acquire a *least upper bound* and a *greatest lower bound* of access to labeled objects based on their assigned lattice positions. Lattice-based access controls were originally developed to address information flow, which is primarily concerned with confidentiality. One common example of a lattice-based access control is a mandatory access control.

Access Control Techniques

3- Lattice-Based Access Controls

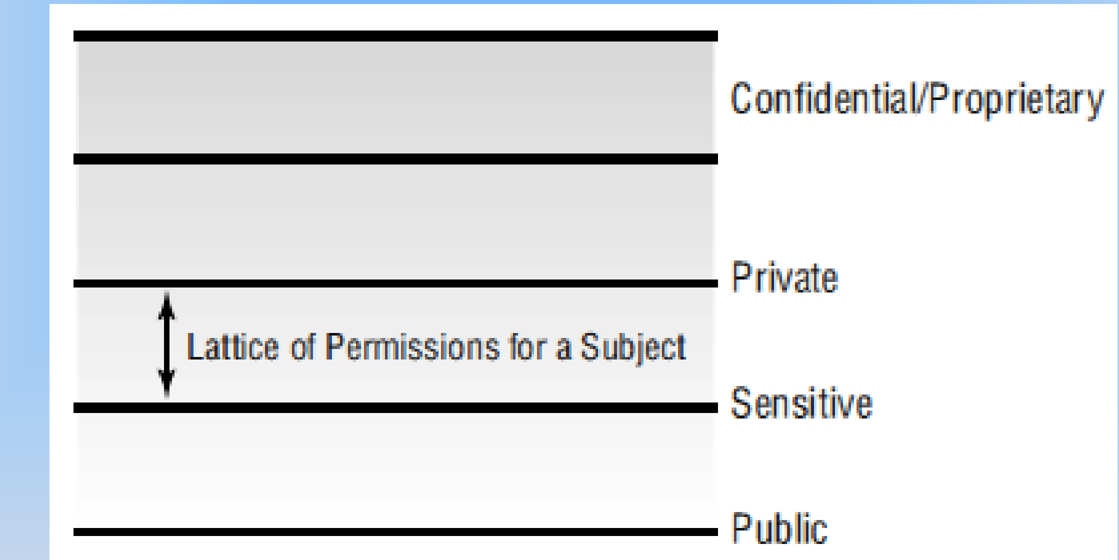


FIGURE 1 .3 A representation of the boundaries provided by lattice-based access controls

Access Control Methodologies and Implementation

There are two primary access control methodologies: ***centralized and decentralized*** (or distributed).

Centralized access control ***implies that all authorization verification is performed by a single entity within a system.***

Decentralized access control, ***or distributed access control, implies that authorization verification is performed by various entities located throughout a system***.

Access Control Methodologies and Implementation

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).***

Access Control Methodologies and Implementation

Centralized and Decentralized Access Control

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; in addition, 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.

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**. As they relate to access control administration, these principles transform into **three main responsibilities:**

* ***User account management***

* ***Activity tracking***

* ***Access rights and permissions management***

Access Control Administration

Account Administration

User account management involves ***creating, maintaining, and closing user accounts***. Although these activities may seem mundane, they are essential to a system's access control capabilities. **Without properly defined and maintained user accounts, a system is unable to establish identity, perform authentication, provide authorization, or track accountability**.

Access Control Administration

Account Administration

Creating New Accounts

Creating new user accounts is a simple process, 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 <u>classification</u> or <u>security level</u> to 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 is 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.**

Access Control Administration

Account Administration

Creating New Accounts

As part of the hiring process, **new employees should be trained on organization security policies and procedures**. Before hiring is complete, **employees must sign an agreement committing to uphold the organization's security standards**. 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 conducted.

Access Control Administration

Account Administration

Creating New Accounts

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 in your secured system.

Access Control Administration

Account Administration

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 conduct 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 those 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.

Access Control Administration

Account Administration

Account Maintenance

When employees leave an organization, their user accounts 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 specific expiration dates programmed into their user accounts**. This maintains a degree of control established at the time of account creation without requiring ongoing administrative oversight.

Access Control Administration

Account Administration

Account, Log, and Journal Monitoring

Activity auditing, account tracking, and system monitoring are also important aspects of access control management. Without these capabilities, it is impossible 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. We discuss auditing and monitoring as an aspect of operations security and as an essential element in a secure environment in Chapter 14, "Auditing and Monitoring."

Access Control Administration

Account Administration

Account, Log, and Journal Monitoring

User accounts, event logs, and system journals help piece together the state of affairs for a server at any referenced point along the timeline of its operation.

Event logs and system journals capture events, **changes**, **messages**, and **other data that describe what activities occurred on a system**. Thus, they are commonly used to support conclusions drawn about any incidents that might warrant investigation. When an account is obtained after an outside **attacker exploits a vulnerable service**, you can bet the server documented some aspects of that incident in its **event logs** and **system journals**.

Access Control Administration

Account Administration

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 to a few specific subjects.

For instance, the data entry department of any given example organization does not require explicit access to the resources and information found in the accounting department. Therefore, not all subjects (those in data entry) require access to particular objects (in this case, accounting). Only managers within the accounting department may access financial data, and only supervisors are responsible for creating and maintaining that data.

Access Control Administration

Account Administration

The Principle of Least Privilege

The principle of least privilege arises from the complex structure that results when subjects are granted access to objects. **This principle states that subjects should be granted only as much access to objects as 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.*** The principle of least privilege is most often linked with DAC, but this concept applies to all types of access control environments, including Non-DAC, MAC, RBAC, and TBAC.

Access Control Administration

Account Administration

The Principle of Least Privilege

Keep in mind that the idea of privilege usually means the ability to write, create, alter, or delete data. Thus, limiting and controlling privilege based upon this concept **can be a protection mechanism for data integrity**. If users can change only those data files that their work tasks require them to change, then the integrity of all other files in the environment is protected.

This principle relies on that **all users have a distinctly defined job description**. Without a specific job description, it is not possible to know what privileges a user does or does not need.

Access Control Administration

Account Administration

Need-to-Know Access

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.

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**.

Access Control Administration

Account Administration

Need-to-Know Access

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.

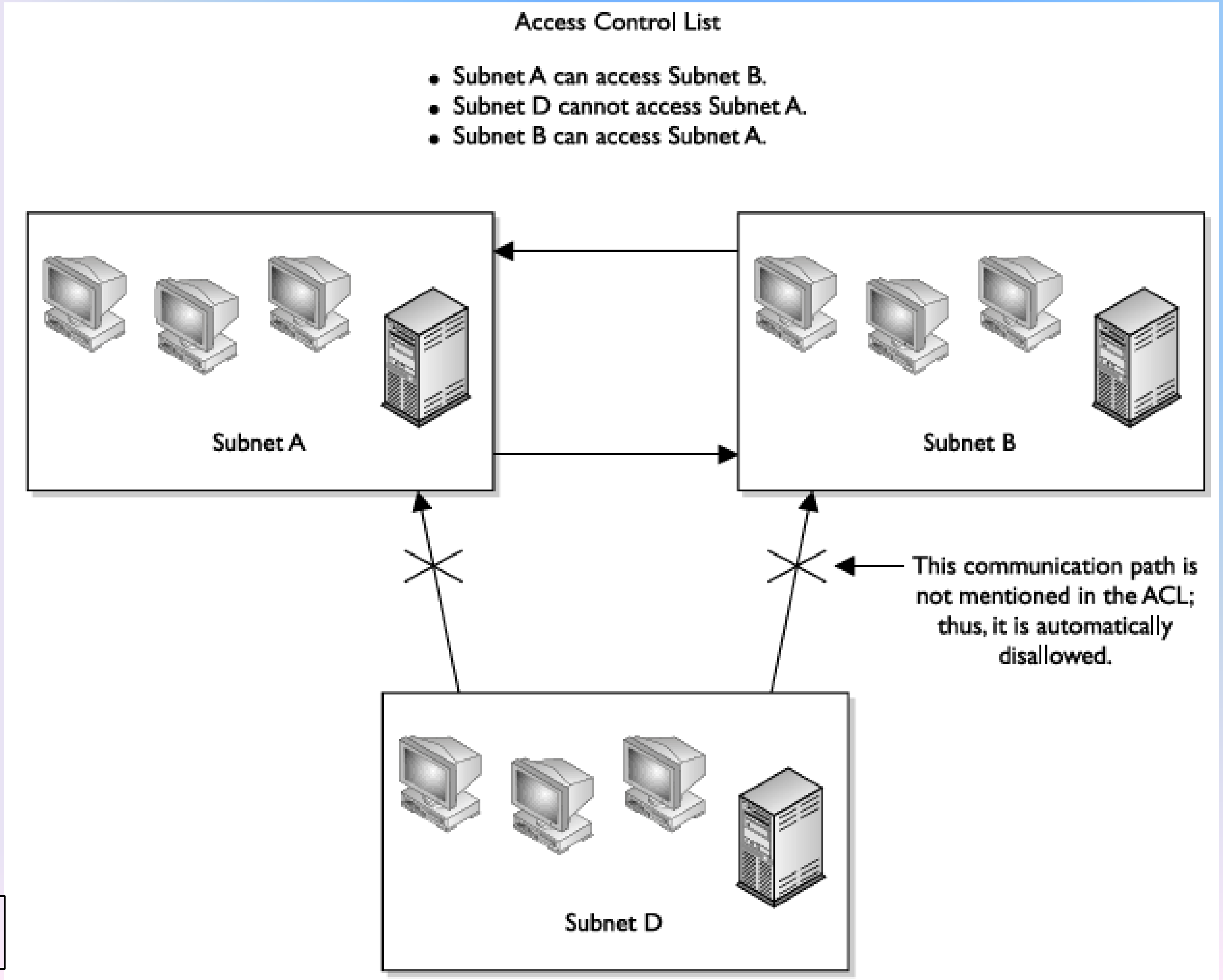
Thus, the criteria for establishing or defining access can be based on identity, roles, rules, classifications, location, time, interfaces, need-to-know, and so on.

Access control models are formal descriptions of a *security policy*, which is a document that encapsulates the security requirements of an organization and prescribes the steps necessary to achieve the desired security. Access control models (or security models) are **used in security evaluations and assessments** as well as **in tools used to validate security**.

Access Control Administration

Account Administration

Need-to-Know Access


Access Control List

- Subnet A can access Subnet B.
- Subnet D cannot access Subnet A.
- Subnet B can access Subnet A.

This communication path is not mentioned in the ACL; thus, it is automatically disallowed.

What is not explicitly allowed should be implicitly denied

Access Control Administration

Account Administration

Excessive Privilege and Creeping Privileges

It’s important to guard against **two problems related to access control**: excessive privilege and creeping privileges.

Excessive privilege **is when a user has more access, privilege, or permission than their assigned work tasks dictate**. If a user account is discovered to have excessive privilege, **the additional and unnecessary privileges should be immediately revoked**.

Creeping privileges **involve a user account accumulating privileges over time as job roles and assigned tasks change**. This can occur because new tasks are added to a user’s job and the related or necessary privileges are added as well but no privileges are ever removed, even if the related work task is no longer associated with or assigned to the user. **Creeping privileges result in excessive privilege.**

You can prevent both of these issues by properly applying the principle of least privilege.

Access Control Administration

Account Administration

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 properly storing and protecting 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**.

Access Control Administration

Account Administration

Separation of Duties and Responsibilities

The 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.**

Access Control Administration

Account Administration

Separation of Duties and Responsibilities

This **separation of duties creates a checks-and-balances system where multiple subjects verify each other's actions and must work in concert to accomplish necessary work tasks.**

Separating duties makes **perpetration 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 agrees to keep a secret. This typically serves as a significant deterrent rather than as a means to corrupt a group en masse. **The separation of duties can be static or dynamic**.

The ***static separation of duties*** **is accomplished by assigning privileges based on written policies that don't change often**.

The ***dynamic separation of duties*** **is used when security requirements cannot be determined until the system is active and functioning.**

Access Control Administration

Account Administration

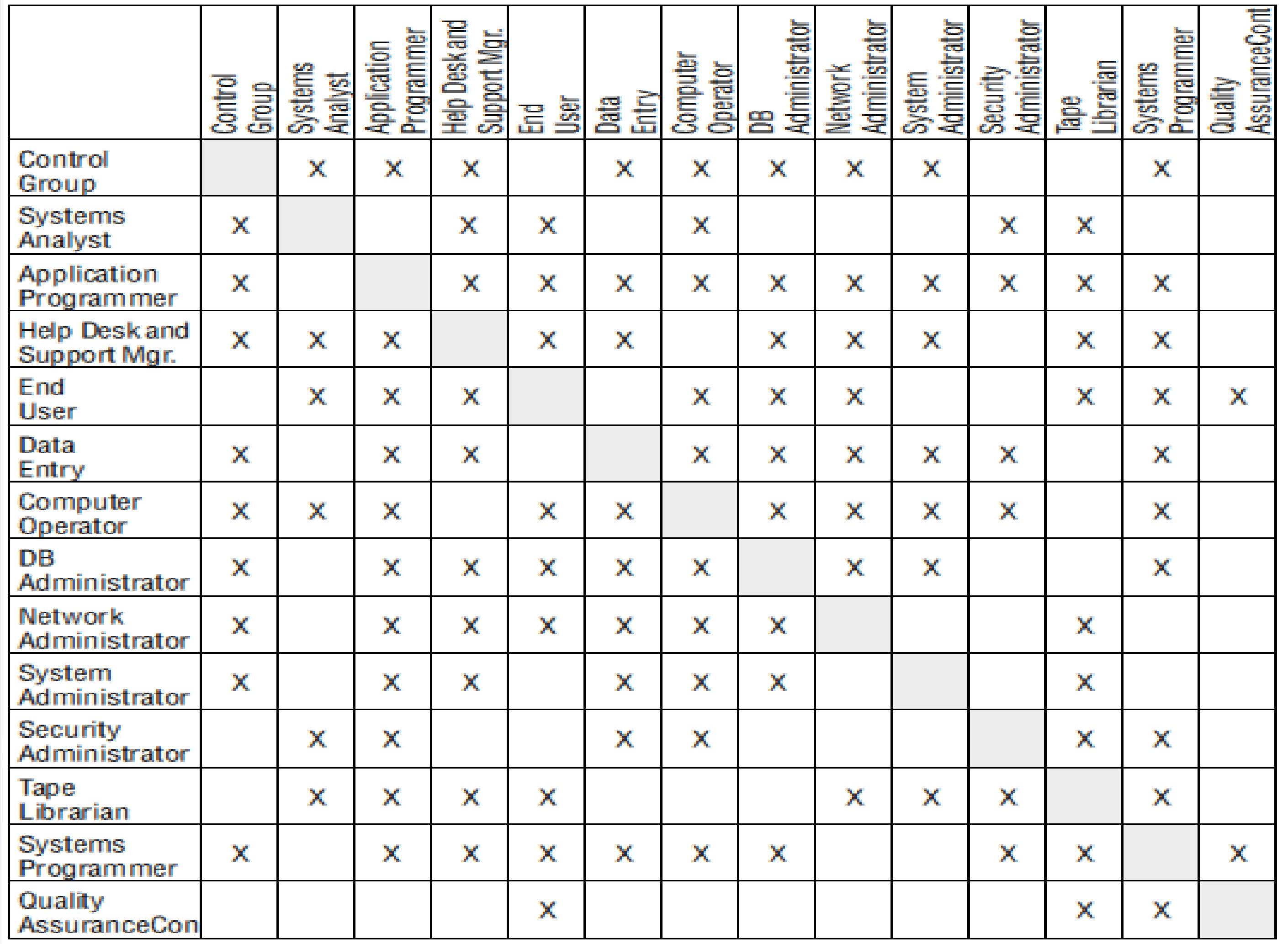
Separation of Duties and Responsibilities

An example of a properly enforced separation of duties is to prevent the security administrator from being able to access system administration utilities or to perform changes to system configuration not related to security. For example, a security administrator needs no more than read access to **system logs**. In this manner, a separation of duties helps prevent conflicts of interest in the types of privileges assigned to administrators as well as users in general. Figure 1.4 illustrates common privileges that should not be combined with others in order to properly enforce a separation of duties.

Access Control Administration

Account Administration

Separation of Duties and Responsibilities



	Control Group	Systems Analyst	Application Programmer	Help Desk and Support Mgr.	End User	Data Entry	Computer Operator	DB Administrator	Network Administrator	System Administrator	Security Administrator	Tape Librarian	Systems Programmer	Quality AssuranceCont
Control Group		X	X	X		X	X	X	X	X			X	
Systems Analyst	X			X	X		X				X	X		
Application Programmer	X			X	X	X	X	X	X	X	X	X	X	
Help Desk and Support Mgr.	X	X	X		X	X		X	X	X		X	X	
End User		X	X	X			X	X	X			X	X	X
Data Entry	X		X	X			X	X	X	X	X		X	
Computer Operator	X	X	X		X	X		X	X	X	X		X	
DB Administrator	X		X	X	X	X	X		X	X			X	
Network Administrator	X		X	X	X	X	X	X				X		
System Administrator	X		X	X		X	X	X				X		
Security Administrator		X	X			X	X					X	X	
Tape Librarian		X	X	X	X				X	X	X		X	
Systems Programmer	X		X	X	X	X	X	X			X	X		X
Quality AssuranceCon					X							X	X	

FIG U RE 1 .4 A segregation of duties control matrix

X—Combination of these functions may create a potential control weakness.