UNIT III

CYBER SECURITY FOR BUSINESS APPLICATIONS AND NETWORKS

Authentication Mechanisms

System Access

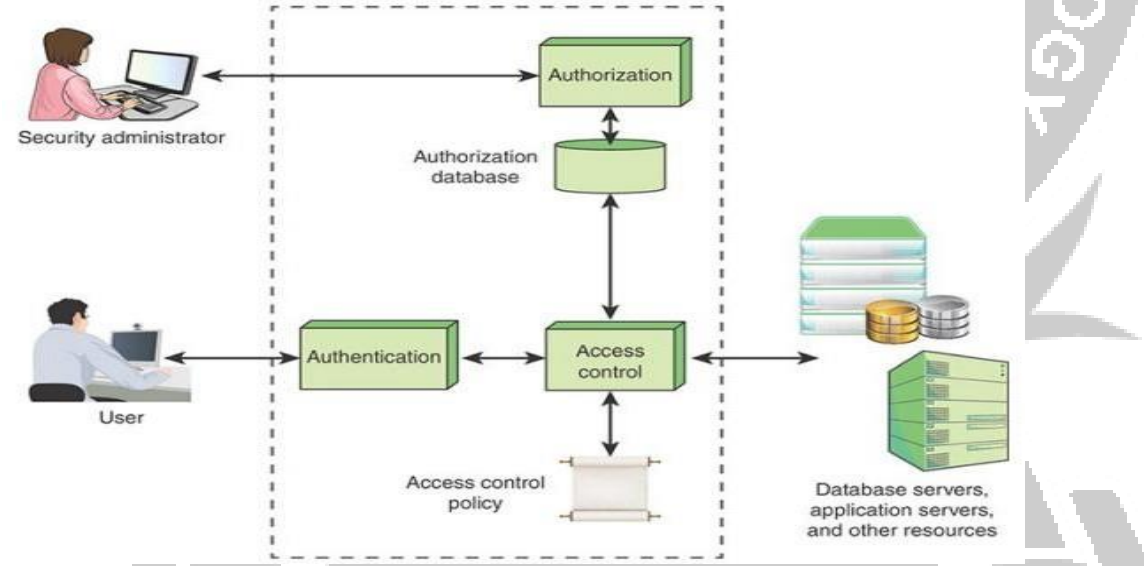
System access is the capability that restricts access to business applications, mobiledevices, systems, and networks to authorized individuals for specific business purposes. System access comprises three distinct functions:

Authentication: Verifying the identity of a user, process, or device, often as aprerequisite to allowing access to resources in an information system. This function is often referred to as user authentication, to distinguish it from message authentication or data authentication.

Authorization: In the context of system access, authorization is the granting of access or other rights to a user, program, or process to access system resources. Authorization defines what an individual or program can do after successful authentication.

Access control: The process of granting or denying specific requests for accessing and using information and related information processing services and for enteringspecific physical facilities. Access control ensures that access to assets is authorizedand restricted based on business and security requirements.

The three functions are shown in Figure 10.1.



Authorization:

A designated security administrator is responsible for creating and maintainingthe authorization database. The administrator sets these authorizations on thebasis of the security policy of the organization and the roles and responsibilities of individual employees.

The process for authorizing users should include the following:

- Associating access privileges with uniquely defined individuals, for example by using unique identifiers, such as user IDs.
- Maintaining a central record of access rights granted to a user ID to access information systems and services.
- Obtaining authorization from the owner of the information system or servicefor the use of the information system or service. Separate approval for access rights from management may also be appropriate.
- Applying the principle of least privilege to give each person the minimum access necessary to do his or her job.
- Assigning individual access privileges for resources based on information security levels and classification of information.
- Specifying the networks and networked services to be accessed, such as files and databases.
- Defining requirements for expiration of privileged access rights.
- Ensuring that identifiers are not reused. This means deleting authorizations associated with a user ID when the individual assigned that user ID changes roles or leaves the organization.

User Authentication

- User authentication is one of the most complex and challenging security functions. There are a wide variety of methods of authentication, with associated threats, risks, and countermeasures. This section provides an overview of them.
- The following three sections look at the three general authenticationfactors: password, hardware token, and biometric.

The following three sections look at the three general authentication factors:

In most computer security contexts, user authentication is a fundamental building block and the primary line of defense. User authentication is the basis for most types of access control and for user accountability.

User authentication encompasses two functions:

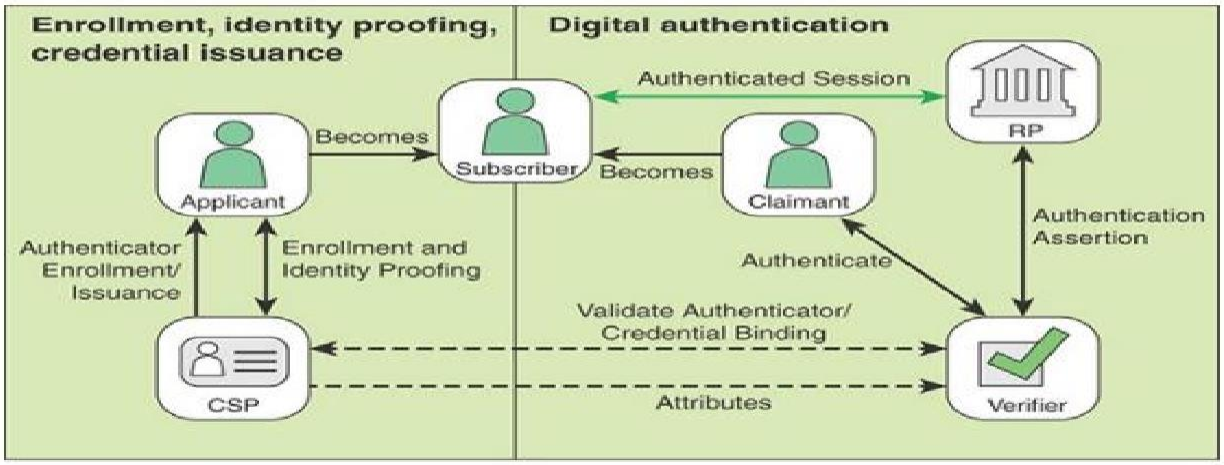
Identification step: This step involves presenting an identifier to the security system. (Assign identifiers carefully because authenticated identities are the basis for other security services, such as access control service.)

Verification step: This step involves presenting or generatingauthentication information that

corroborates the binding between the entity and the identifier.

A Model for Electronic User Authentication

National Institute of Standards and Technology (NIST) SP 800-63, *Digital Identity Guidelines*, defines a general model for user authentication that involves a number of entities and procedures, as shown in Figure 10.2.



CSP = credential service provider
RP = relying party

FIGURE 10.2 The NIST 800-63 Digital Identity Model

Three concepts are important in understanding this model:

Digital identity: The digital identity is the unique representation of a subject engaged in an online transaction. The representation consists of an attribute or set of attributes that uniquely describe a subject within a given context of a digital service but does not necessarily uniquely identify the subject in all contexts.

Identity proofing: This process establishes that a subject is who he or she claimsto be to a stated level of certitude. This process involves collecting, validating, and verifying information about a person.

Digital authentication: This process involves determining the validity of one or more authenticators used to claim a digital identity. Authentication establishes thata subject attempting to access a digital service is in control of the technologies usedto authenticate.

Successful authentication provides reasonable risk-based assurances that the subject accessing the service today is the same as the subject that previously accessed the service.

Six entities are defined in Figure 10.2:

Credential service provider (CSP): A trusted entity that issues or registers subscriber authenticators. For this purpose, the CSP establishes a digital credential for each subscriber and issues electronic credentials to subscribers. A CSP may be an independent third party or may issue credentials for its own use.

Verifier: An entity that verifies the claimant9s identity by verifying the claimant9s possession and control of one or two authenticators, using an authentication protocol. To do this, the verifier may also need to validate

credentials that link the authenticator(s) to the subscriber9s identifier and check their status.

Relying party (RP): An entity that relies upon the subscriber9s authenticator(s) and credentials or a verifier9s assertion of a claimant9s identity, typically to processa transaction or grant access to information or a system.

Applicant: A subject undergoing the processes of enrollment and identity proofing.

Claimant: A subject whose identity is to be verified using one or more authentication protocols.

Subscriber: A party who has received a credential or authenticator from a CSP.

TABLE 10.1 Authentication Factors

Factor	Examples	Properties
Knowledge	User ID Password PIN	Can be shared Many passwords are easy to guess Can be forgotten
Possession	Smart card Electronic badge Electronic key	Can be shared Can be duplicated (cloned) Can be lost or stolen
Inherence	Fingerprint Face Iris Voice print	Not possible to share False positives and false negatives possible Forging difficult

Multifactor Authentication :

Multifactor authentication refers to the use of more than one of the authenticationmeans in the preceding list (see Figure 10.3). The strength of an authentication system is largely determined by the number of factors incorporated by the system.

A system that requires two factors is generally stronger than a system requiring a single factor, assuming that the individual factors are reasonably strong.

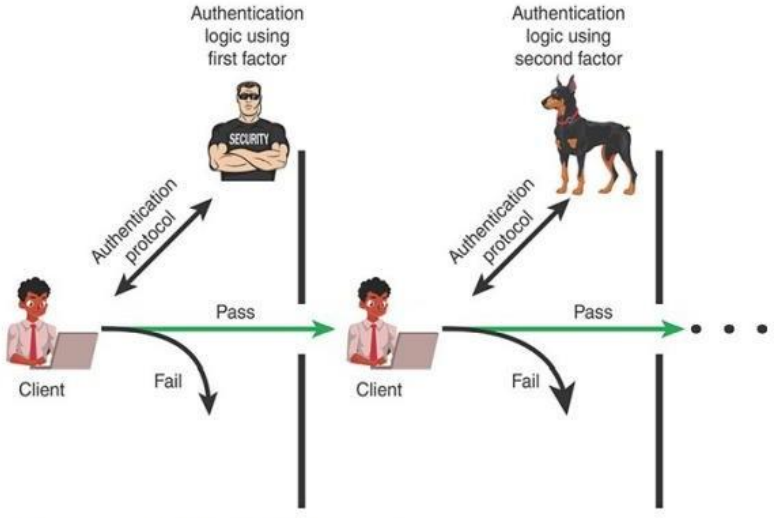


FIGURE 10.3 Multifactor Authentication

Password-Based Authentication :What you know is a widely used line of defense against intruders is a password system. Virtually all multiuser systems, network- based servers, web-based ecommerce sites, and other similar services require that auser provide not only a name or identifier (ID) but also a password.

- ✓ The system compares the password to a previously stored password for that user ID, maintained in a system password file. The password serves to authenticate the ID of the individual logging on to the system.
- ✓ In turn, the ID provides security in the following ways: The ID determines whether the user is authorized to gain access to a system. In some systems, only those who already have an ID filed on the system are allowed to gain access.
- ✓ The ID determines the privileges accorded to the user. A few users may have supervisory or <superuser= status that enables them to read files and performfunctions that are especially protected by the operating system. Some systems have guest or anonymous accounts, and users of these accounts have more limited privileges than others.
- ✓ The ID is used in what is referred to as discretionary access control. For example, by listing the IDs of the other users, a user may grant permission to them to read files owned by that user.

Possession-Based Authentication :Objects that a user possesses for the purpose ofuser authentication are sometimes called hardware tokens

Card Type	Defining Feature	Example
Embossed	Raised characters only, on front	Traditional credit card
Magnetic stripe	Magnetic bar on back, characters on front	Bank card
Memory	Electronic memory inside	Prepaid phone card
Smart ▪ Contact ▪ Contactless	Electronic memory and processor inside ▪ Electrical contacts exposed on surface ▪ Radio antenna embedded inside	Biometric ID card

Types of Cards Used as Possession Factor

eID Functions

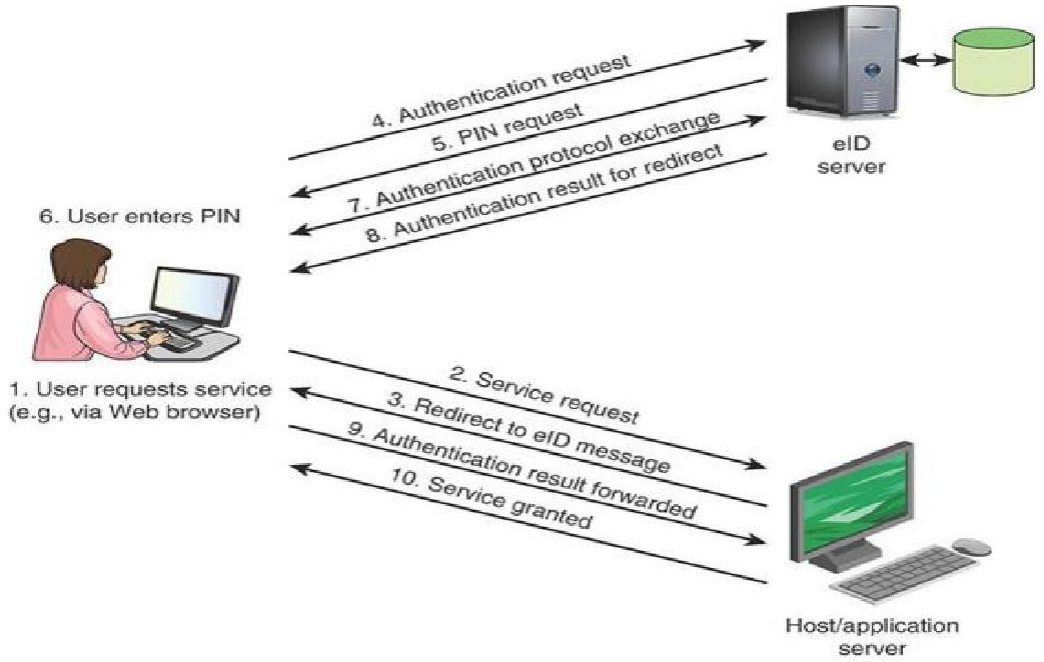


FIGURE 10.6 User Authentication with eID

Biometric Authentication :

A biometric authentication system attempts to authenticate an individual based on his or her unique physical characteristics.

These include both static characteristics (for example, fingerprints, hand geometry, facial characteristics, retinal and iris patterns) and dynamic characteristics (for example, voiceprint, signature).

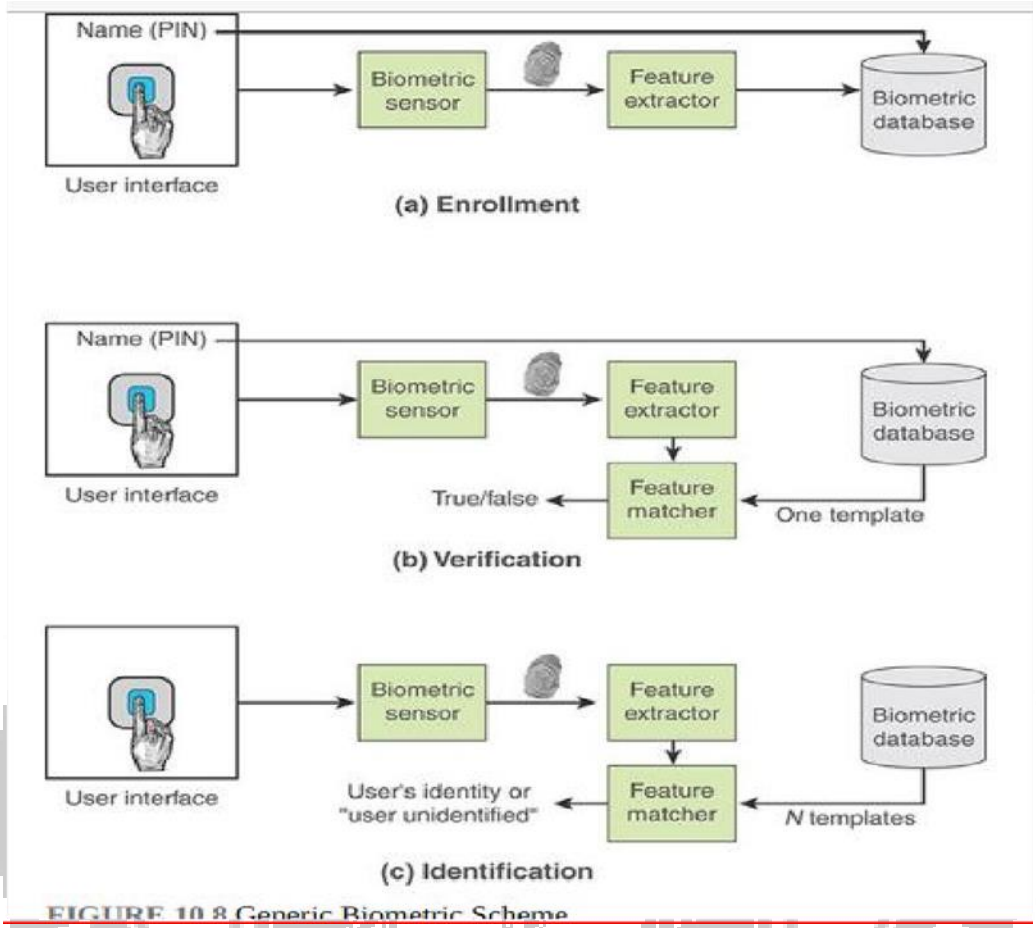


FIGURE 10.8 Generic Biometric Scheme