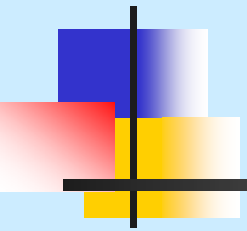


Chapter 3: Security Basics

OBJECTIVES

- Identify the persons responsible for information security
- Describe security principles
- Describe effective authentication methods
- Control access to computer systems
- Audit information security schemes

Identifying Who Is Responsible for Information Security

- When an organization secures its information, it completes a few basic tasks:
  - It must analyze its assets and the threats these assets face from threat agents
  - It identifies its vulnerabilities and how they might be exploited
  - It regularly assesses and reviews the security policy to ensure it is adequately protecting its information

Identifying Who Is Responsible for Information Security (cont.)

- Bottom-up approach: major tasks of securing information are accomplished from the lower levels of the organization upwards
- This approach has one key advantage: the bottom-level employees have the technical expertise to understand how to secure information

Identifying Who Is Responsible for Information Security (cont.)

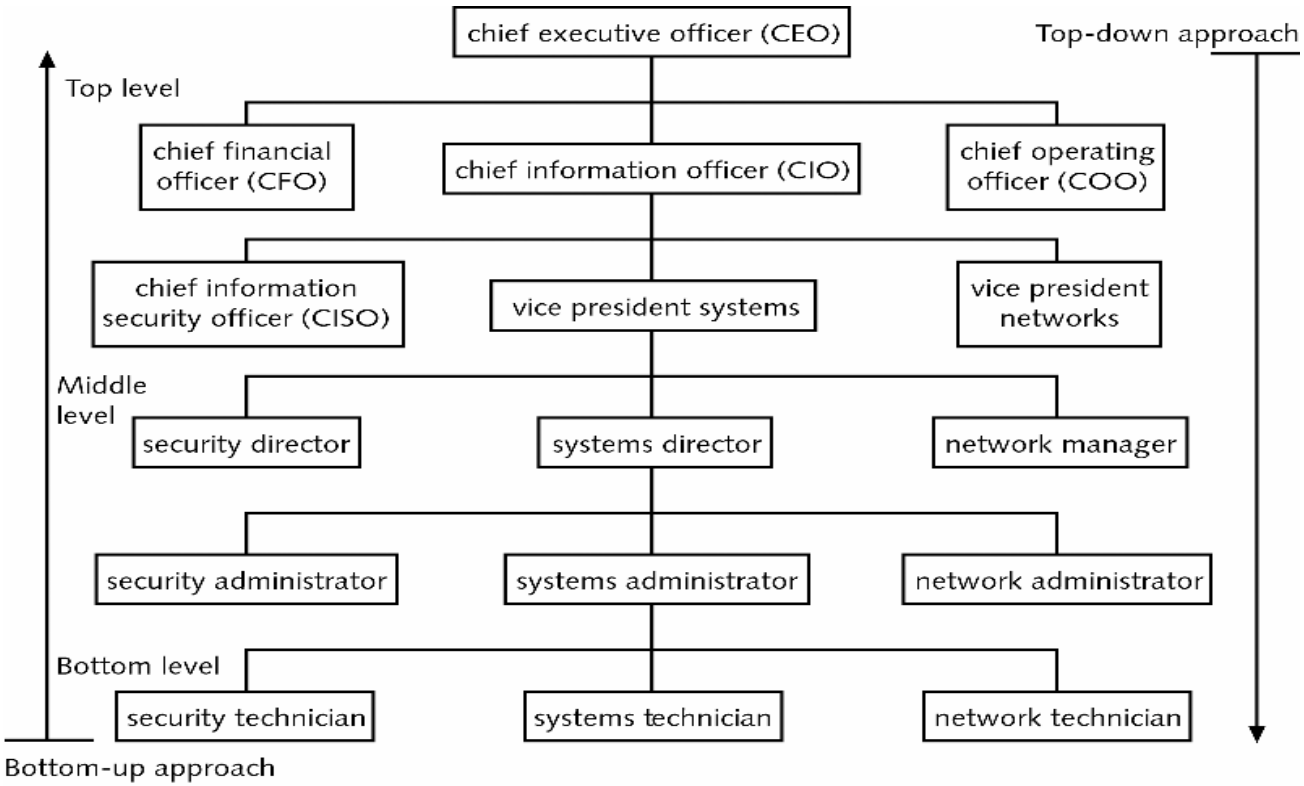


Figure 1 Approaches to organization security

Identifying Who Is Responsible for Information Security (cont.)

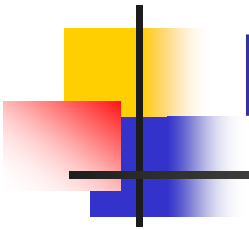
- Top-down approach starts at the highest levels of the organization and works its way down
- A security plan initiated by top-level managers has the backing to make the plan work

Identifying Who Is Responsible for Information Security (cont.)

- Chief information security officer (CISO): helps develop the security plan and ensures it is carried out
- Human firewall: describes the security-enforcing role of each employee

Understanding Security Principles

- Ways information can be attacked:
  - Crackers can launch distributed denial-of-service (DDoS) attacks through the Internet
  - Spies can use social engineering
  - Employees can guess other user's passwords
  - Hackers can create back doors
- Protecting against the wide range of attacks calls for a wide range of defense mechanisms



Layering

- Layered security approach has the advantage of creating a barrier of multiple defenses that can be coordinated to thwart a variety of attacks
- Information security likewise must be created in layers
- All the security layers must be properly coordinated to be effective

Layering (continued)

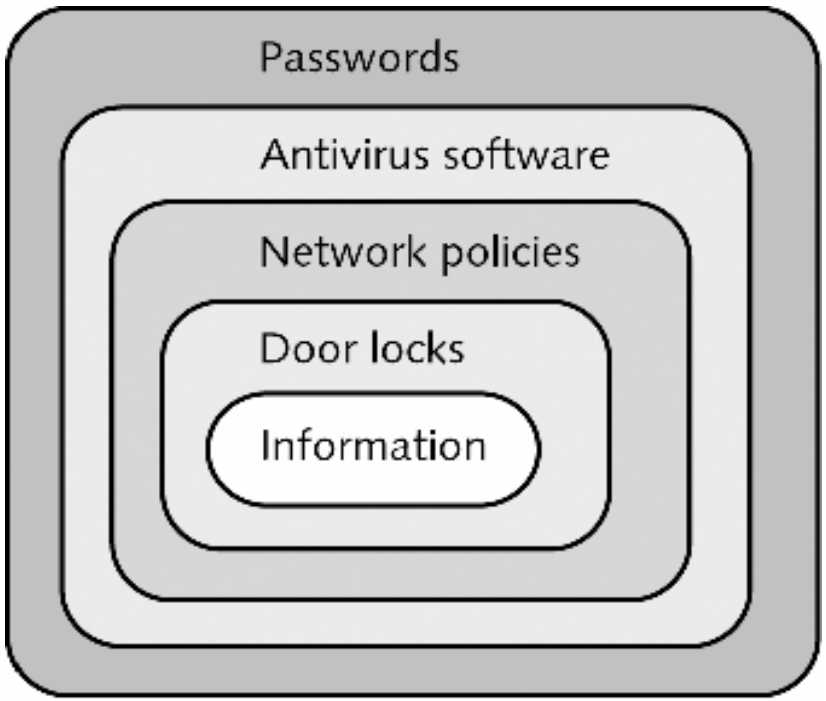
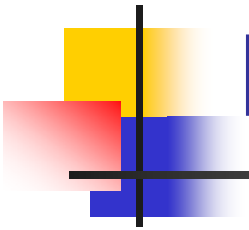


Figure 2 Layered security



Limiting

- Limiting access to information reduces the threat against it
- Only those who must use data should have access to it
- Access must be limited for a subject (a person or a computer program running on a system) to interact with an object (a computer or a database stored on a server)
- The amount of access granted to someone should be limited to what that person needs to know or do

Limiting (continued)

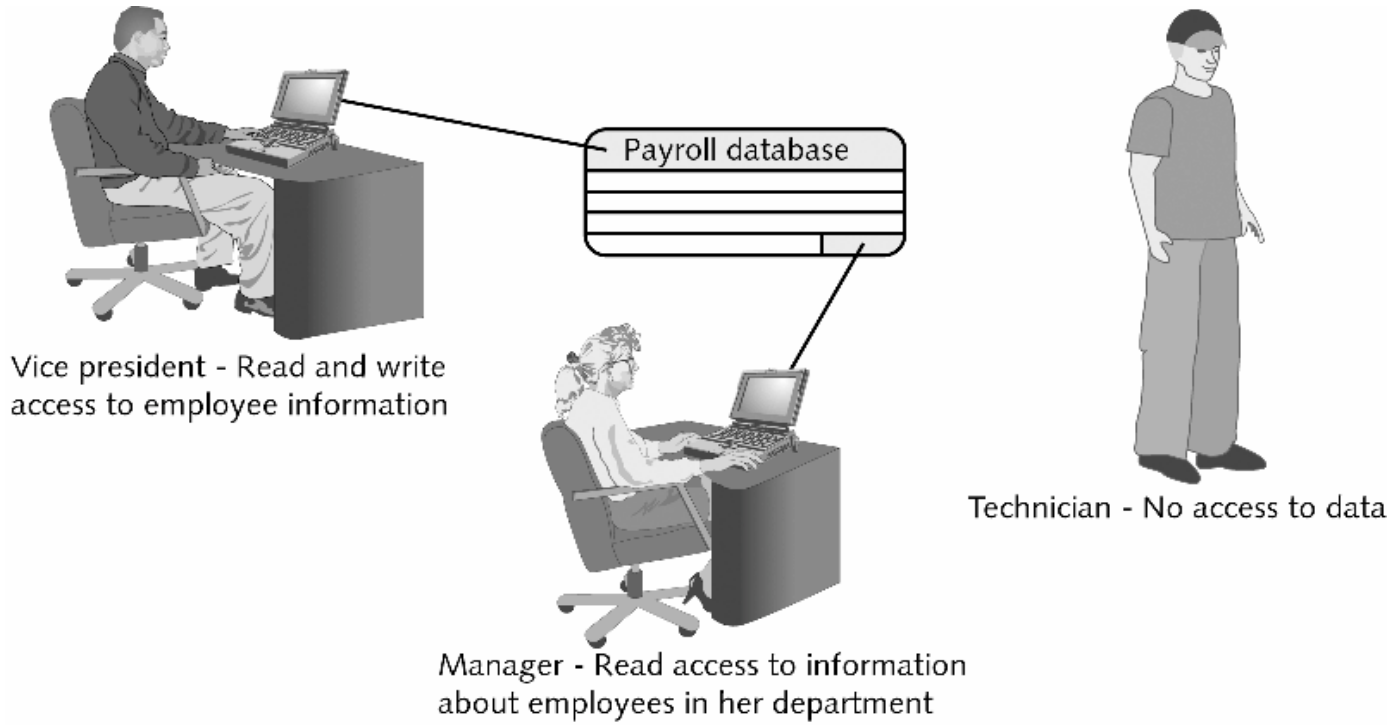
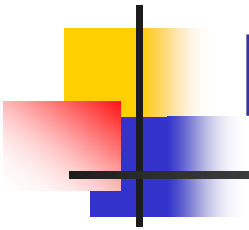


Figure 3 Limiting access to payroll database

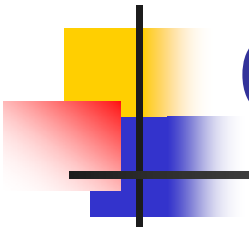


Diversity

- Diversity is closely related to layering
- You should protect data with diverse layers of security, so if attackers penetrate one layer, they cannot use the same techniques to break through all other layers
- Using diverse layers of defense means that breaching one security layer does not compromise the whole system

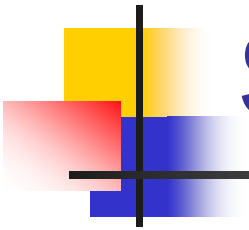
Diversity (cont.)

- You can set a firewall to filter a specific type of traffic, such as all inbound traffic, and a second firewall on the same system to filter another traffic type, such as outbound traffic
- Using firewalls produced by different vendors creates even greater diversity



Obscurity

- Obscuring what goes on inside a system or organization and avoiding clear patterns of behavior make attacks from the outside difficult



Simplicity

- Complex security systems can be difficult to understand, troubleshoot, and feel secure about
- The challenge is to make the system simple from the inside but complex from the outside

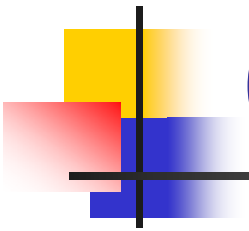
Using Effective Authentication Methods

- Information security rests on three key pillars:
  - Authentication
  - Access control
  - Auditing

Using Effective Authentication Methods (cont.)

- Authentication:
  - Process of providing identity
  - Can be classified into three main categories:
    - something you know ,e.g. password or PIN
    - something you have ,e.g. smart card or an identification device
    - something physically unique to you ,e.g. fingerprint
  - Most common method: providing a user with a unique username and a secret password

Username and Password (cont.)

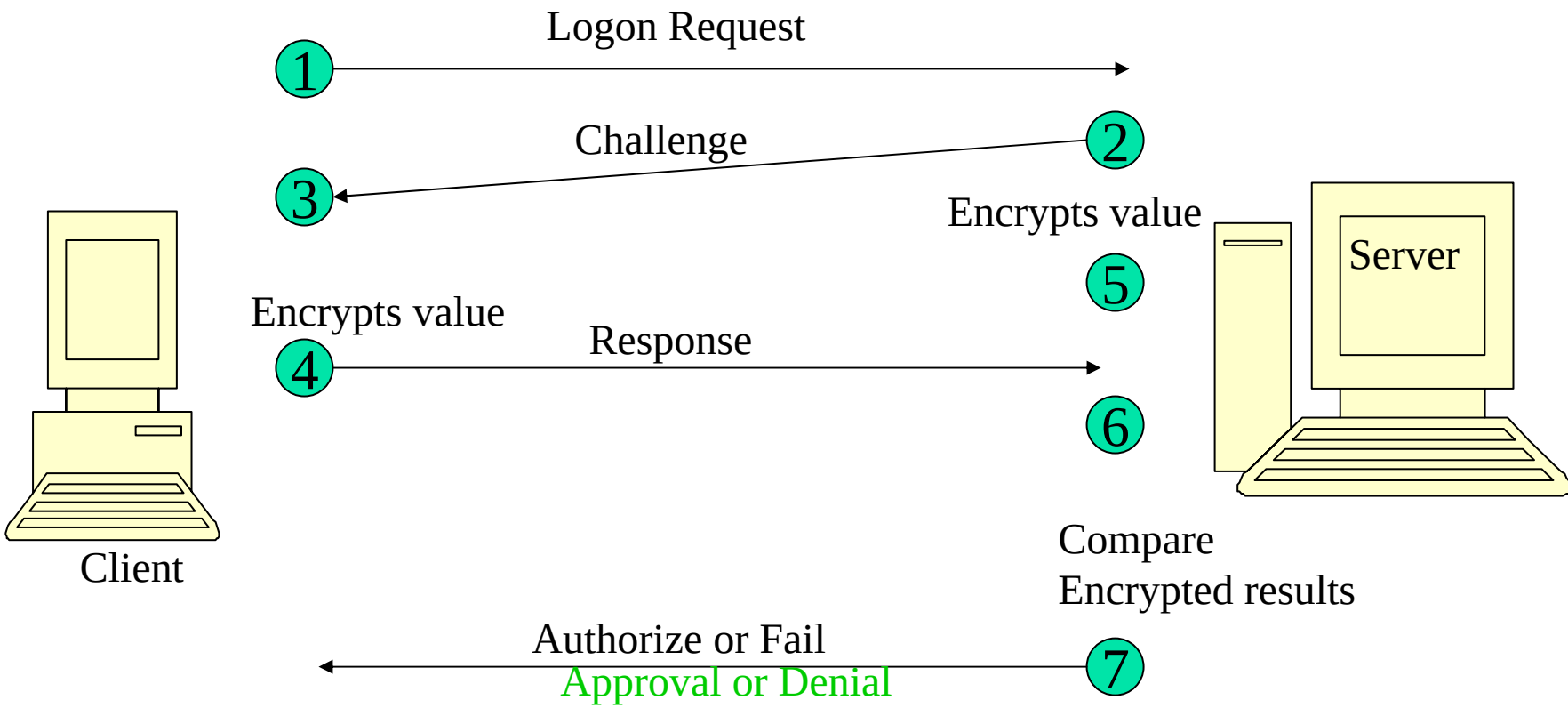


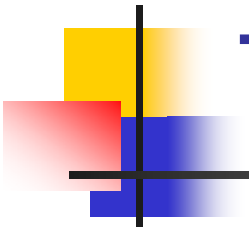
- Password Authentication Protocol (PAP) offers no true security.
- The username and password values are both sent to the server as clear text and checked for a match
- If they match, the user is granted access
- In most modern implementations, PAP is shunned in favor of other more secure authentication methods

Challenge Handshake Authentication Protocol (CHAP)

- Considered a more secure procedure for connecting to a system than using a password
  - User enters a password and connects to a server; server sends a challenge message to user's computer
  - User's computer receives message and uses a specific algorithm (encryption) to create a response sent back to the server
  - Server checks response by comparing it to its own calculation of the expected value; if values match, authentication is acknowledged; otherwise, connection is terminated

CHAP Authentication

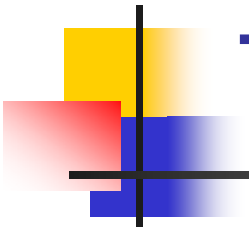




Tokens

Token :security device that authenticates the user by having the appropriate permission embedded into the token itself

- Security tokens are similar to certificates
- They contain the rights and access privileges of the token bearer as part of the token.
- Passwords are based on what you know, tokens are based on what you have
- Proximity card: plastic card with an embedded, thin metal strip that emits a low-frequency, short-wave radio signal



Tokens (cont.)

- The authentication system creates a token every time a user connects or a session begins
- At the completion of a session the token is destroyed

Biometrics

- Uses a person's unique characteristics to authenticate them
- Is an example of authentication based on what you are
- Human characteristics that can be used for identification include:
  - Fingerprint
  - Face
  - Hand
  - Iris
  - Retina
  - Voice

Biometrics (continued)

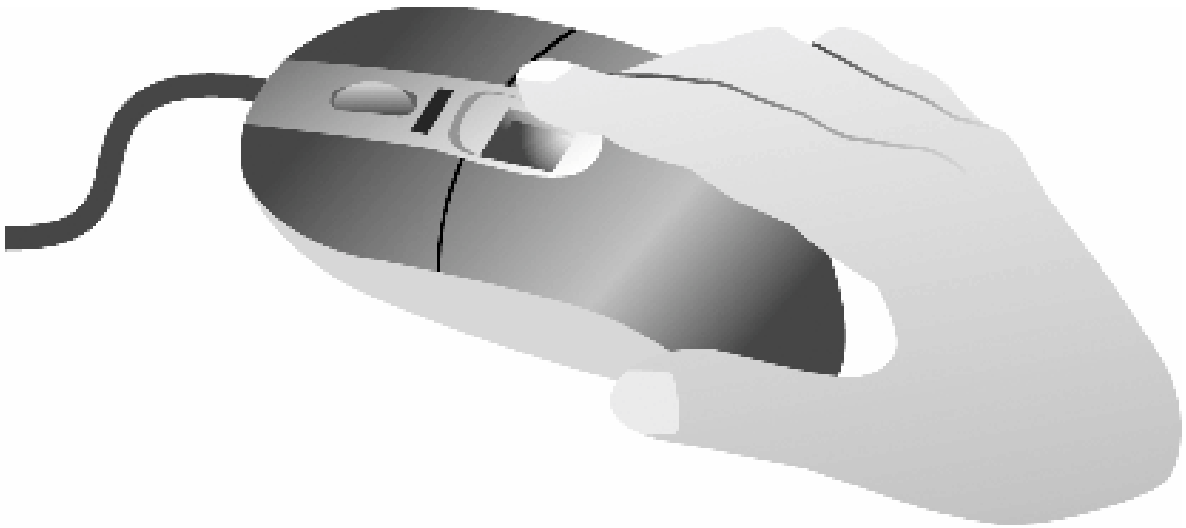
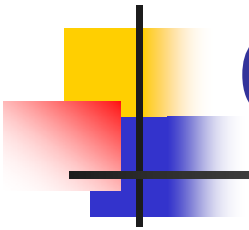


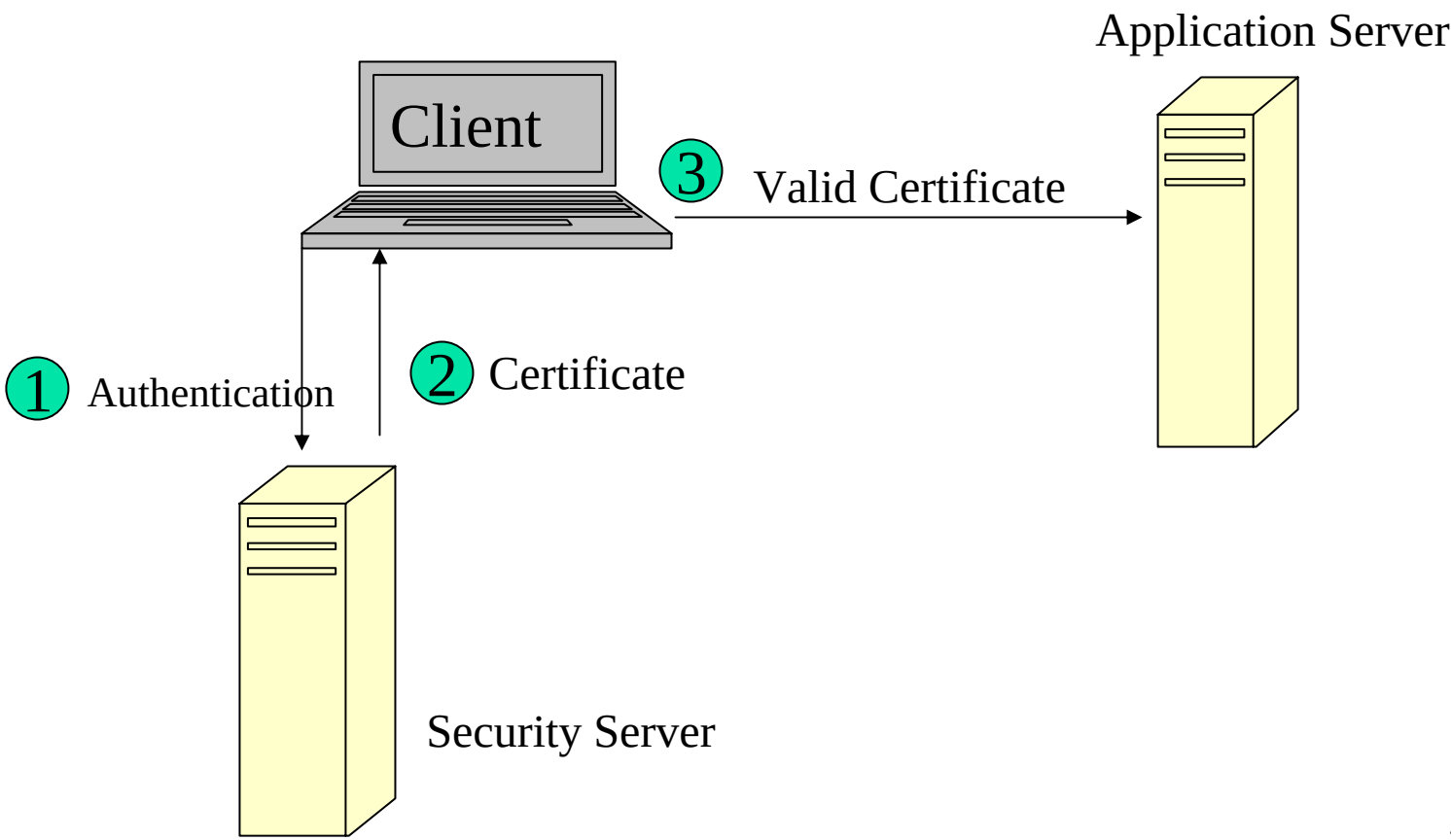
Figure 4 Fingerprint scanner

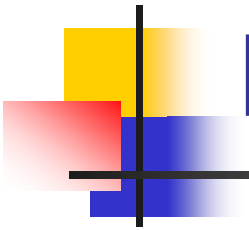


Certificates

- The key system does not prove that the senders are actually who they claim to be
- Certificates let the receiver verify who sent the message
- Certificates link or bind a specific person to a key
- A server or certification authority (CA) can issue a certificate that will be accepted by the challenging system
- Digital certificates are issued by a certification authority (CA), an independent third-party organization
- If you have a certificate then you can prove to the system that you are who you say you are and are authenticated to work with the resources

CERTIFICATE BEING ISSUED ONCE IDENTIFICATION HAS BEEN VERIFIED





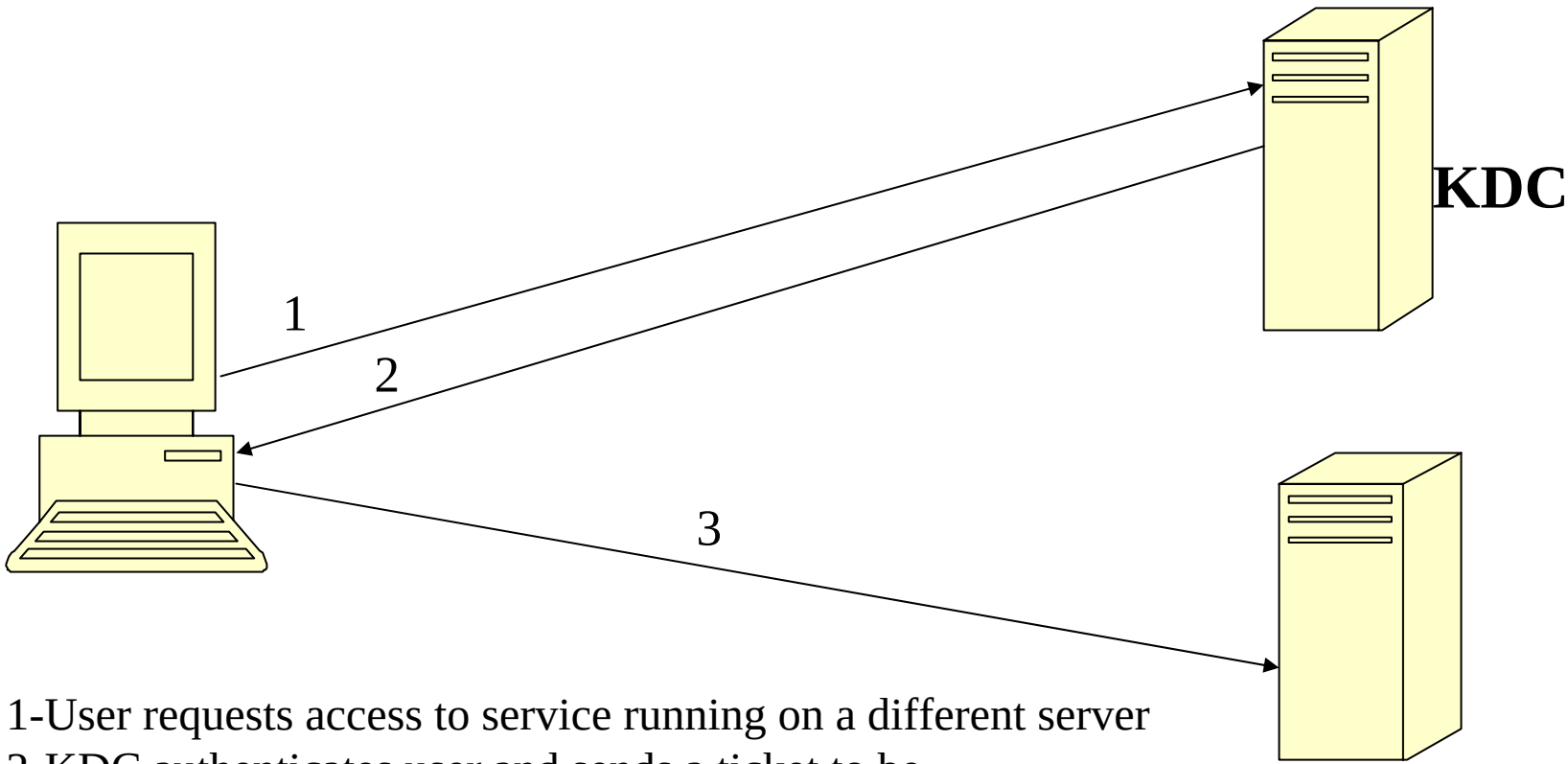
Kerberos

- Authentication system developed by the Massachusetts Institute of Technology (MIT)
- Used to verify the identity of networked users, like using a driver's license to cash a check
- Typically used when someone on a network attempts to use a network service and the service wants assurance that the user is who he says he is

Kerberos (cont.)

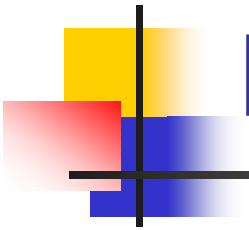
- A state agency, such as the DMV, issues a driver's license that has these characteristics:
  - It is difficult to copy
  - It contains specific information (name, address, height, etc.)
  - It lists restrictions (must wear corrective lenses, etc.)
  - It expires on a specified date
- The user is provided a ticket that is issued by the Kerberos authentication server (AS), much as a driver's license is issued by the DMV

Kerberos (cont.)



1-User requests access to service running on a different server
2-KDC authenticates user and sends a ticket to be
used between the user and the service on the server
3-User's workstation sends a ticket to the service

Server Providing
services to the user



Mutual Authentication

- Two-way authentication (mutual authentication) can be used to combat identity attacks, such as man-in-the-middle and replay attacks
- The server authenticates the user through a password, tokens, or other means

Mutual Authentication (continued)

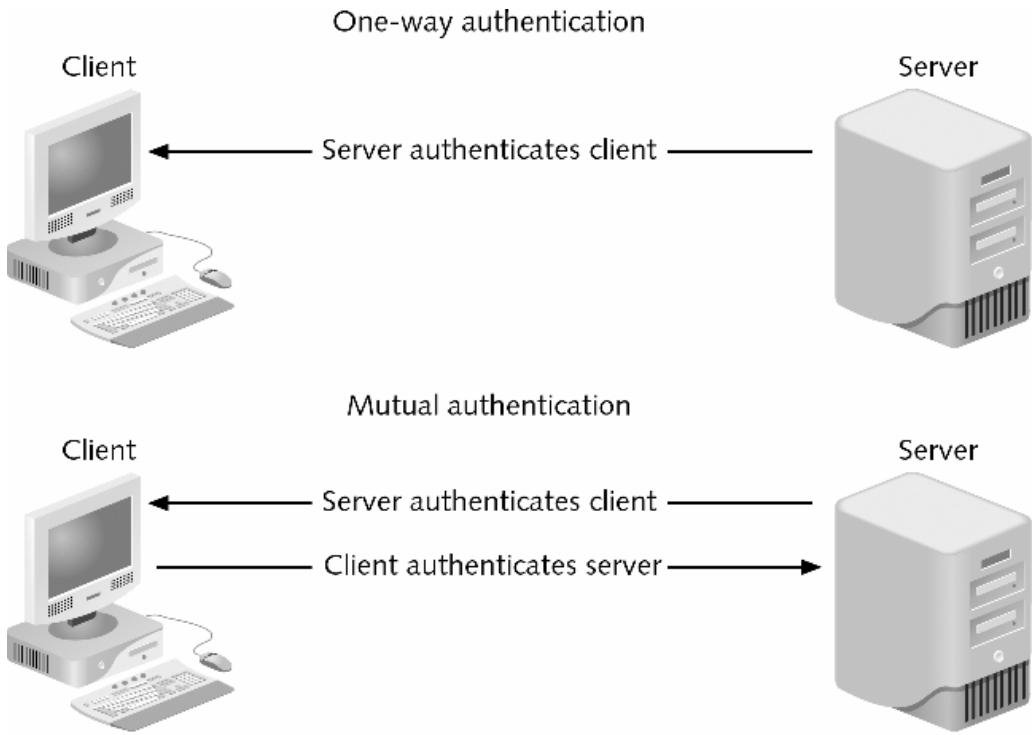


Figure 5 Mutual authentication

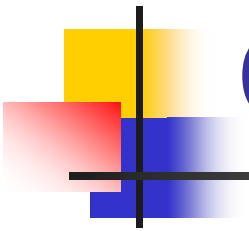
Multifactor Authentication

- Multifactor authentication: implementing two or more types of authentication
- A system that uses smart cards and passwords is referred to as multi-factor authentication system
- Being strongly proposed to verify authentication of cell phone users who use their phones to purchase goods and services

Smart Card

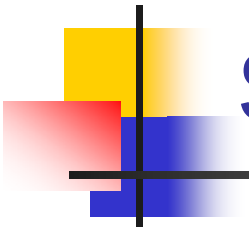
- A smart card is a type of badge or card that gives you access to resources, including buildings, parking lots, and computers
- It contains information about your identity and access privileges
- Each area or computer has a card scanner or reader in which you insert your card
- The reader is connected to the workstation and validates against the security system
- This increases the security of the authentication because you must be in physical possession of the smart card to use the resources.

Controlling Access to Computer Systems



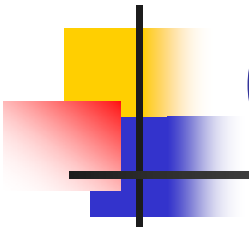
- Restrictions to user access are stored in an access control list (ACL)
- An ACL is a table in the operating system that contains the access rights each subject (a user or device) has to a particular system object (a folder or file)

Controlling Access to Computer Systems (continued)



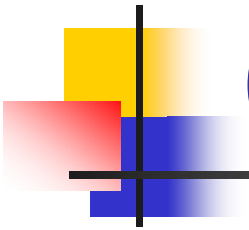
- In Microsoft Windows, an ACL has one or more access control entries (ACEs) consisting of the name of a subject or group of subjects
- Inherited rights: user rights based on membership in a group

Mandatory Access Control (MAC)



- A more restrictive model
- The subject is not allowed to give access to another subject to use an object
- MAC is a static model that uses a predefined set of access privileges to files on the system.
- The system administrators establish these parameters and associates them with an account, files, or resources
- Administrators are the only people who can change access
- MAC uses *labels* to identify the level of sensitivity that applies to objects

Role Based Access Control (RBAC)



- Instead of setting permissions for each user or group, you can assign permissions to a position or role and then assign users and other objects to that role
- Users and objects inherit all of the permissions for the role
- Users can be assigned roles system wide and can then perform certain functions or duties based on the roles they're assigned
- E.g. a role called salesperson. Can access the information established for that role from any station in the network, based strictly on his role
- The RBAC model is common in network administrative roles

Discretionary Access Control (DAC)

- Least restrictive model
- Type of access most users associate with their personal computers
- DAC model allows the owner of a resource to establish privileges to the information they own.
- The difference between DAC and MAC is that labels are not mandatory but can be applied as needed
- The DAC model allows a user to share a file or use a file that someone else has shared.
- It establishes an access control list (ACL) that identifies the users who have authorization to that information
- This allows the owner to grant or revoke access to individuals or groups of individuals based on the situation
- This model is dynamic in nature and allows information to be shared easily between users

Auditing Information Security Schemes

- Two ways to audit a security system
  - Logging records which user performed a specific activity and when
  - System scanning to check permissions assigned to a user or role; these results are compared to what is expected to detect any differences