UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Fakulti Teknologi Maklumat dan Komunikasi

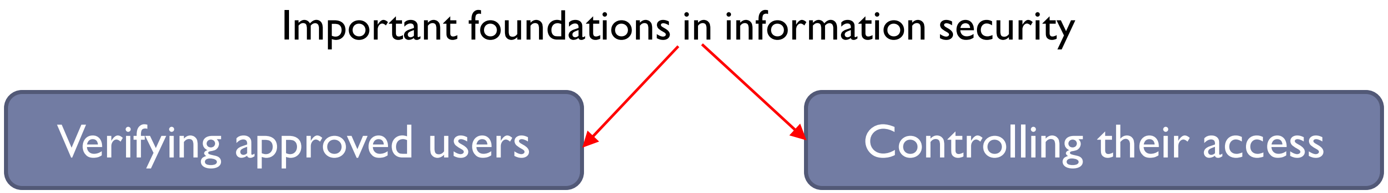
Data Communication and Networking

Lecture 10: Access Control Fundamentals

Objectives

- Define access control and list the four access control models
- Describe logical access control methods
- Explain the different types of physical access control
- Define authentication services

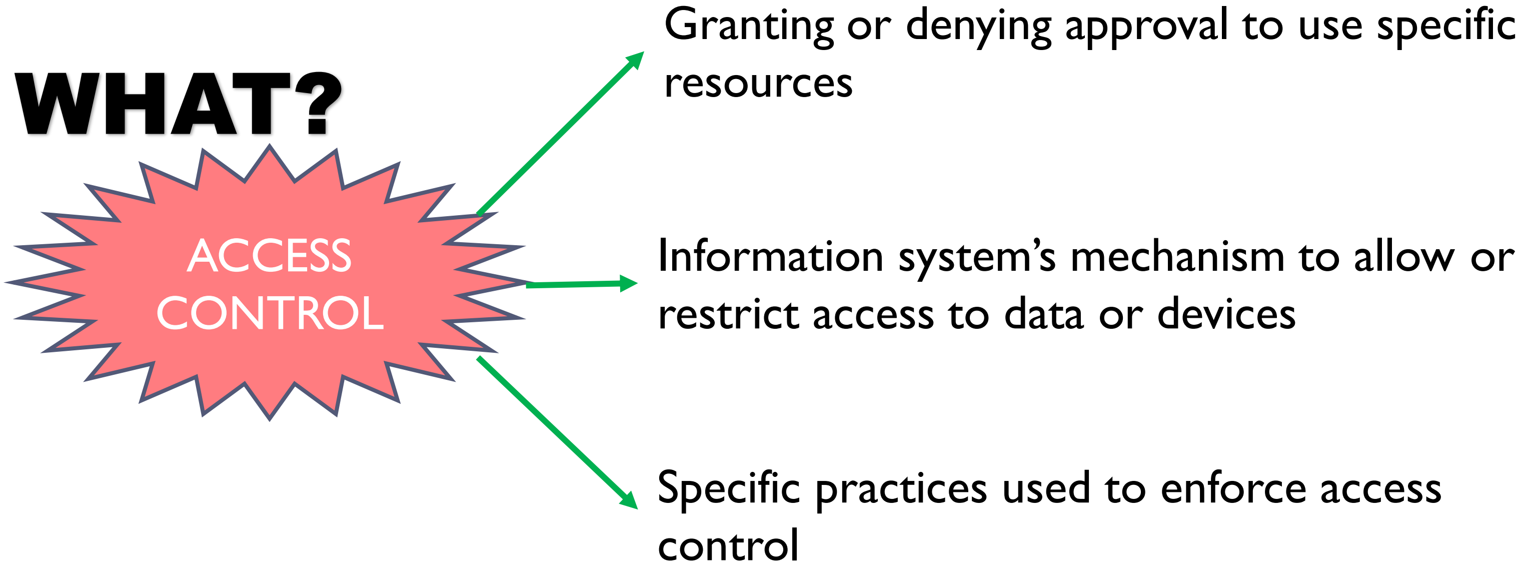
Introduction



Important foundations in information security

Verifying approved users

Controlling their access



WHAT?

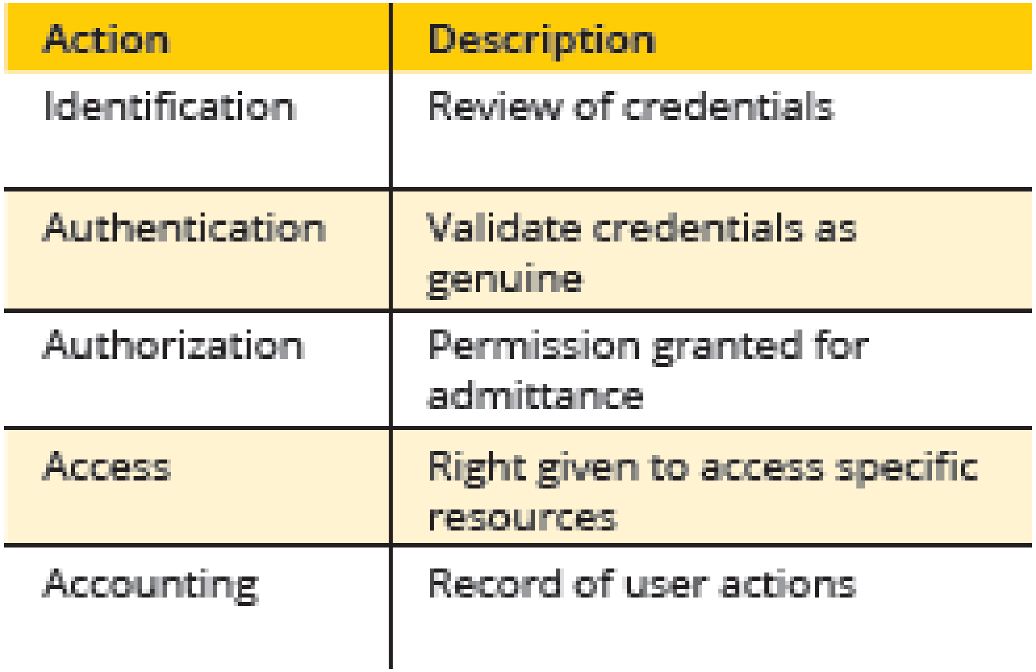
ACCESS CONTROL

Granting or denying approval to use specific resources

Information system's mechanism to allow or restrict access to data or devices

Specific practices used to enforce access control

Access Control Terminology

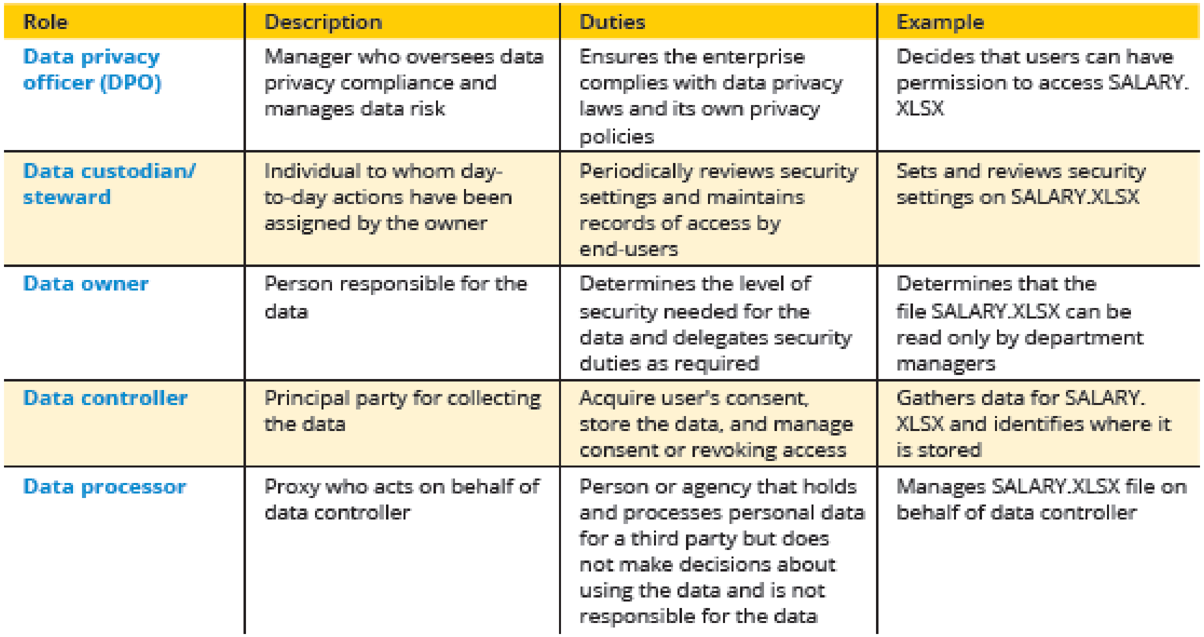


Action	Description
Identification	Review of credentials
Authentication	Validate credentials as genuine
Authorization	Permission granted for admittance
Access	Right given to access specific resources
Accounting	Record of user actions

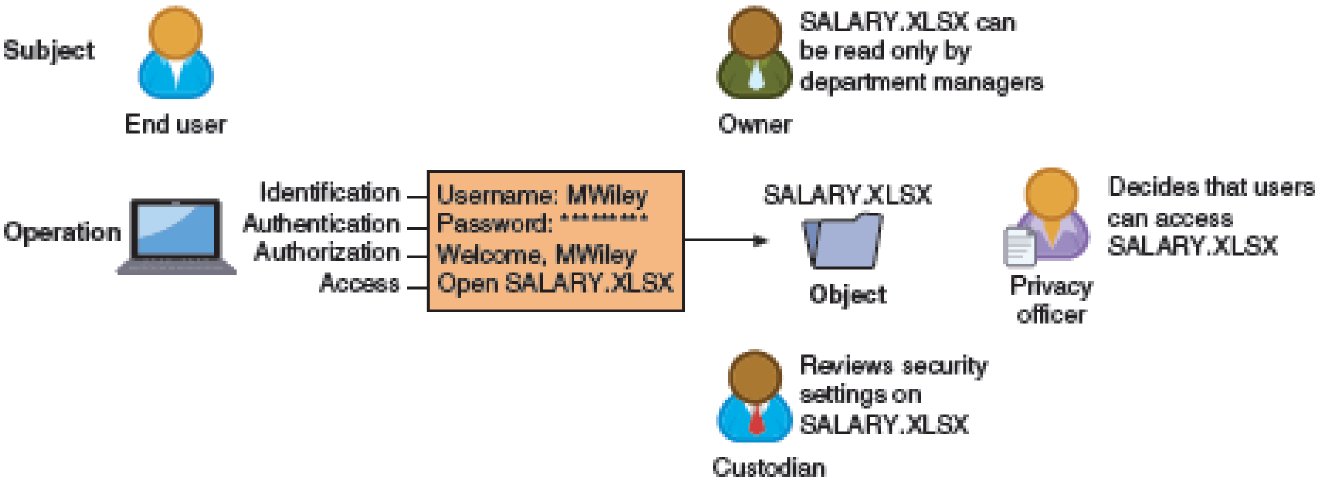
Basic steps in access control

Access Control Terminology

- *Object*. An object is a specific resource, such as a file or a hardware device.
- *Subject*. A subject is a user or a process functioning on behalf of the user that attempts to access an object.
- *Operation*. The action that is taken by the subject over the object is called an operation. For example, a user (subject) may attempt to delete (operation) a file (object).



Role	Description	Duties	Example
Data privacy officer (DPO)	Manager who oversees data privacy compliance and manages data risk	Ensures the enterprise complies with data privacy laws and its own privacy policies	Decides that users can have permission to access SALARY.XLSX
Data custodian/steward	Individual to whom day-to-day actions have been assigned by the owner	Periodically reviews security settings and maintains records of access by end-users	Sets and reviews security settings on SALARY.XLSX
Data owner	Person responsible for the data	Determines the level of security needed for the data and delegates security duties as required	Determines that the file SALARY.XLSX can be read only by department managers
Data controller	Principal party for collecting the data	Acquire user's consent, store the data, and manage consent or revoking access	Gathers data for SALARY.XLSX and identifies where it is stored
Data processor	Proxy who acts on behalf of data controller	Person or agency that holds and processes personal data for a third party but does not make decisions about using the data and is not responsible for the data	Manages SALARY.XLSX file on behalf of data controller

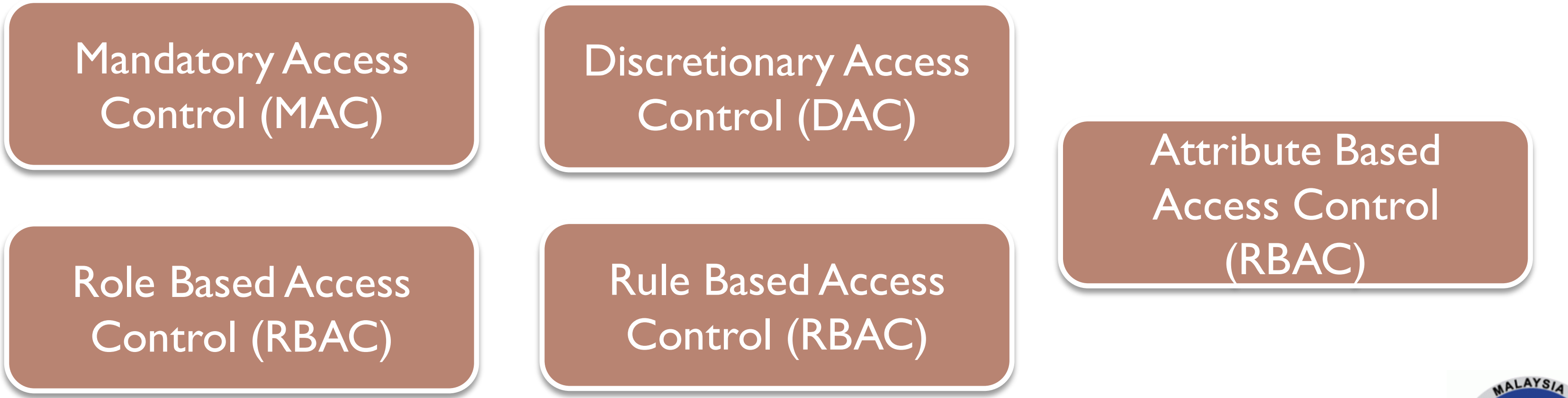


Technical access control and terminology

Access Control Models

- Standards that provide a predefined framework for hardware or software developers
- Used to implement access control in a device or application
- Custodians can configure security based on owner's requirements

- Five major access control models



Mandatory Access Control (MAC)

Discretionary Access Control (DAC)

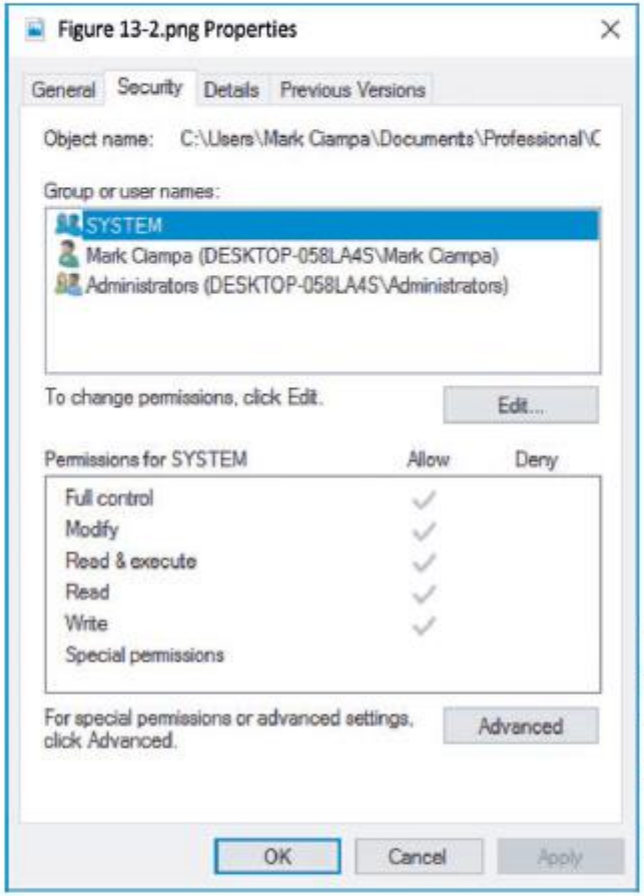
Attribute Based Access Control (RBAC)

Role Based Access Control (RBAC)

Rule Based Access Control (RBAC)

Access Control Models: Discretionary Access Control (DAC)

- Least restrictive model
- Every object has an owner
- Owners have total control over their objects
- Owners can give permissions to other subjects over their objects



Object name: C:\Users\Mark Ciampa\Documents\Professional\C

Group or user names:

- SYSTEM
- Mark Ciampa (DESKTOP-058LA4S\Mark Ciampa)
- Administrators (DESKTOP-058LA4S\Administrators)

To change permissions, click Edit.

Permissions for SYSTEM	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

For special permissions or advanced settings, click Advanced.

Windows Discretionary Access Control (DAC)

Access Control Models: Discretionary Access Control (DAC)

DAC weaknesses

- Relies on decisions by end user to set proper security level
- Incorrect permissions may be granted
- Subject's permissions will be "inherited" by any programs the subject executes

Access Control Models: Mandatory Access Control (MAC)

- Most restrictive access control model
- Typically found in military settings
- Two elements
    - Labels
    - Levels
- MAC grants permissions by matching object labels with subject labels
    - Labels indicate level of privilege
- To determine if file may be opened:
    - Compare object and subject labels
    - Subject must have equal or greater level than object to be granted access

Access Control Models: Role Based Access Control (RBAC)

- Also called Non-discretionary Access Control
- Access permissions are based on user's job function
- RBAC assigns permissions to particular roles in an organization
  - –Users are assigned to those roles

Access Control Models: Rule Based Access Control (RB-RBAC)

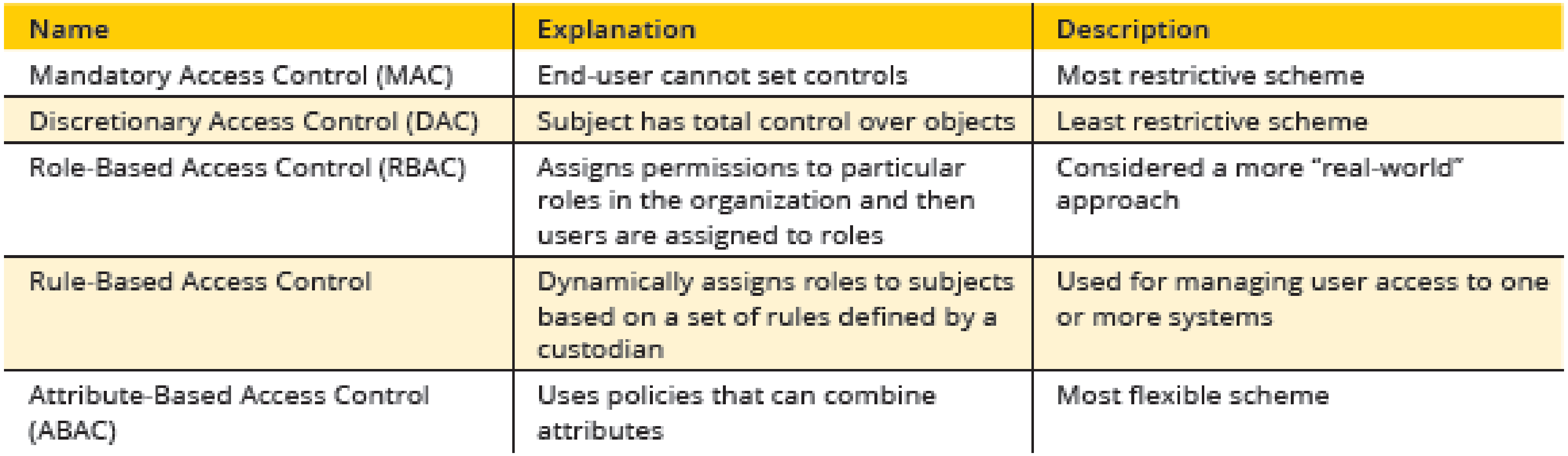
- Dynamically assigns roles to subjects based on a set of rules defined by a custodian
- Each resource object contains access properties based on the rules
- When user attempts access, system checks object's rules to determine access permission
- Often used for managing user access to one or more systems

  -Business changes may trigger application of the rules specifying access changes

Access Control Models: Attribute-Based Access Control (ABAC)

- Flexible policies that can combine attributes.
- Can be formatted using an If-Then-Else structure,

Access Control Models

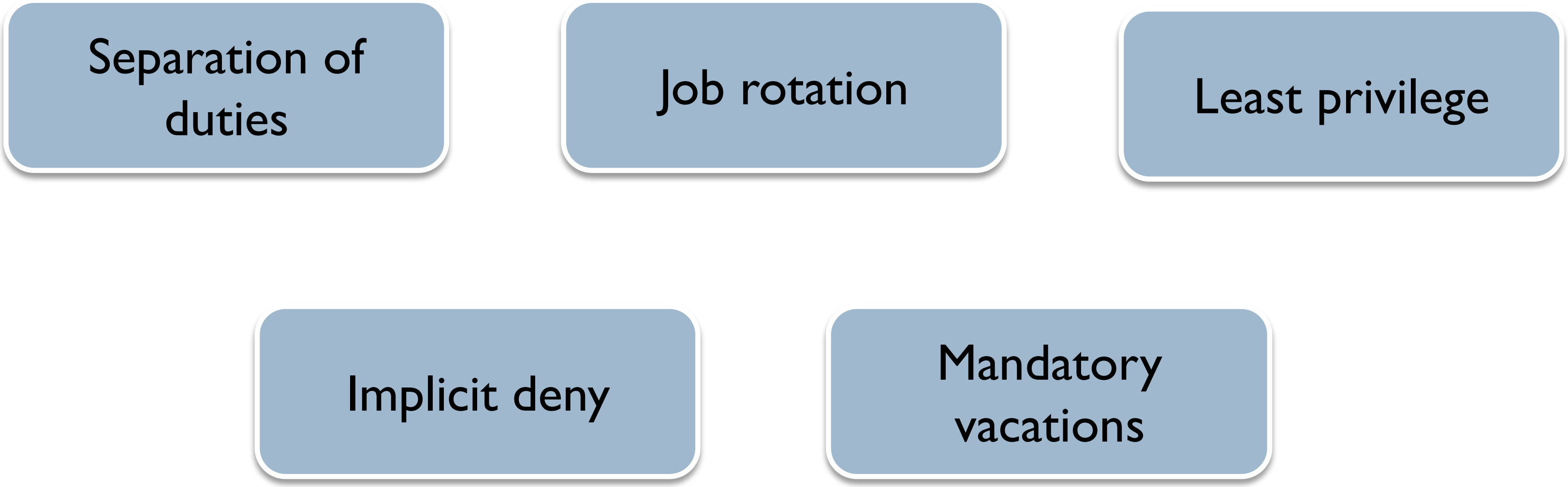


Name	Explanation	Description
Mandatory Access Control (MAC)	End-user cannot set controls	Most restrictive scheme
Discretionary Access Control (DAC)	Subject has total control over objects	Least restrictive scheme
Role-Based Access Control (RBAC)	Assigns permissions to particular roles in the organization and then users are assigned to roles	Considered a more "real-world" approach
Rule-Based Access Control	Dynamically assigns roles to subjects based on a set of rules defined by a custodian	Used for managing user access to one or more systems
Attribute-Based Access Control (ABAC)	Uses policies that can combine attributes	Most flexible scheme

Access control models

Best Practices for Access Control

- Establishing best practices for limiting access can help secure systems and data
- Examples of best practices



Separation of duties

Job rotation

Least privilege

Implicit deny

Mandatory vacations

Best Practices for Access Control: Separation of Duties

- Fraud can result from single user being trusted with complete control of a process
- Requiring two or more people responsible for functions related to handling money
- System is not vulnerable to actions of a single person

Best Practices for Access Control: Job Rotation

- Individuals periodically moved between job responsibilities
- Employees can rotate within their department or across departments

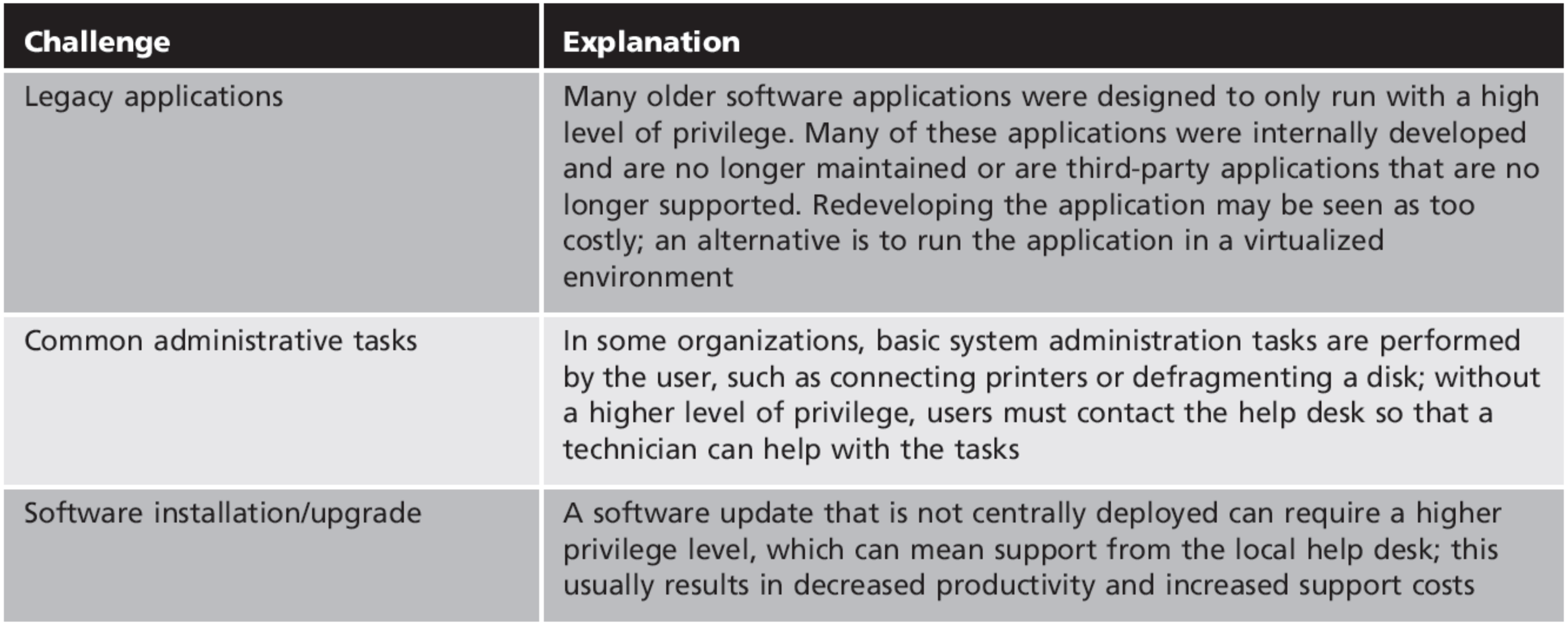
ADVANTAGES

- Limits amount of time individuals are in a position to manipulate security configurations
- Helps expose potential avenues for fraud

  -Individuals have different perspectives and may uncover vulnerabilities
- Reduces employee burnout

Best Practices for Access Control: Least Privilege

- Limiting access to information based on what is needed to perform a job function
- Helps reduce attack surface by eliminating unnecessary privileges
- Should apply to users and processes on the system
- Processes should run at minimum security level needed to correctly function
- Temptation to assign higher levels of privilege is great



Challenge	Explanation
Legacy applications	Many older software applications were designed to only run with a high level of privilege. Many of these applications were internally developed and are no longer maintained or are third-party applications that are no longer supported. Redeveloping the application may be seen as too costly; an alternative is to run the application in a virtualized environment
Common administrative tasks	In some organizations, basic system administration tasks are performed by the user, such as connecting printers or defragmenting a disk; without a higher level of privilege, users must contact the help desk so that a technician can help with the tasks
Software installation/upgrade	A software update that is not centrally deployed can require a higher privilege level, which can mean support from the local help desk; this usually results in decreased productivity and increased support costs

Challenges of least privilege

Best Practices for Access Control: Implicit Deny

- If a condition is not explicitly met, access request is rejected
- Example: network router rejects access to all except conditions matching the rule restrictions

Best Practices for Access Control: Mandatory Vacations

- Limits fraud, because perpetrator must be present daily to hide fraudulent actions
- Audit of employee's activities usually scheduled during vacation for sensitive positions

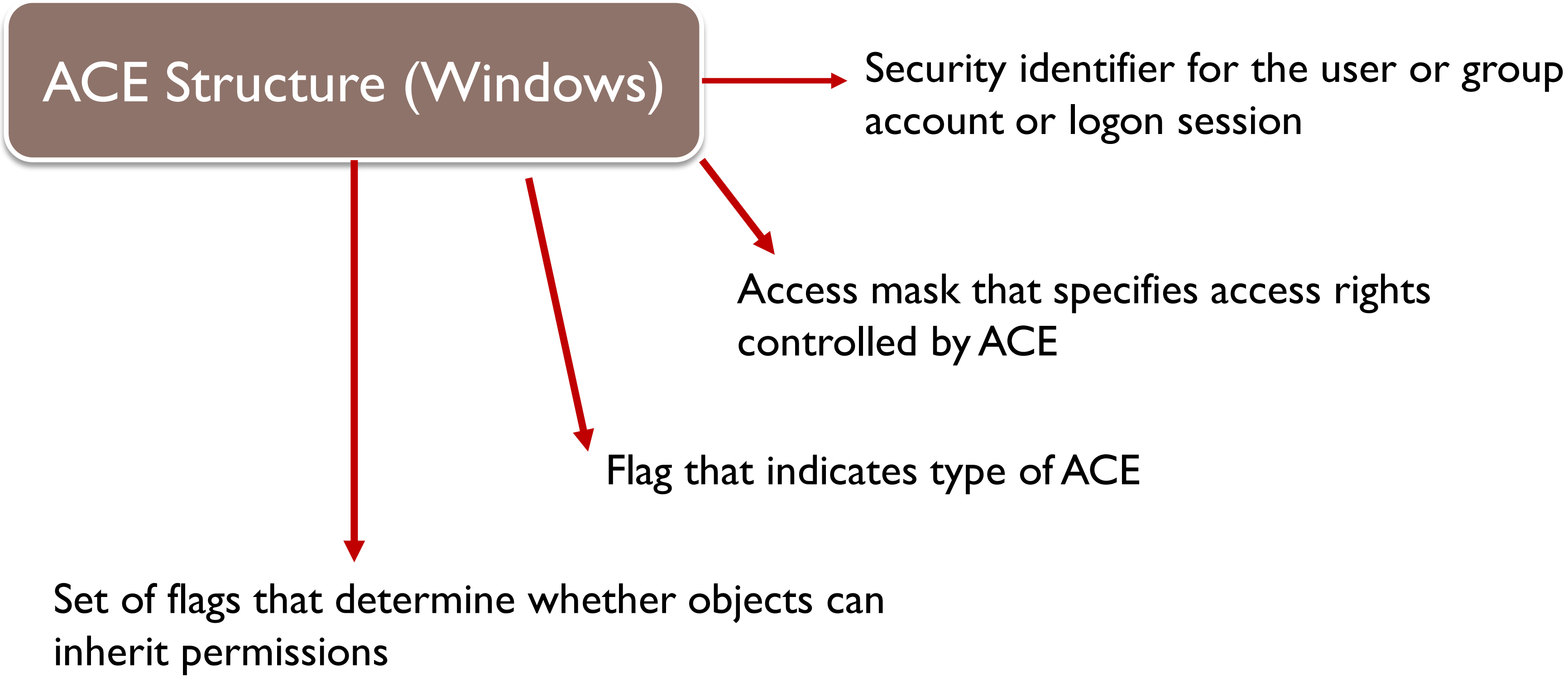
Access Control Lists (ACL)

- Set of permissions attached to an object
- Specifies which subjects may access the object and what operations they can perform
- When subject requests to perform an operation:

  -System checks ACL for an approved entry
- ACLs usually viewed in relation to operating system files

Access Control Lists (ACL)

- Each entry in the ACL table is called access control entry (ACE)



ACE Structure (Windows)

Security identifier for the user or group account or logon session

Access mask that specifies access rights controlled by ACE

Flag that indicates type of ACE

Set of flags that determine whether objects can inherit permissions

Group Policies

- Microsoft Windows feature
  - –Provides centralized management and configuration of computers and remote users using Active Directory (AD)
  - –Usually used in enterprise environments
  - –Settings stored in Group Policy Objects (GPOs)

- Local Group Policy
  - –Fewer options than a Group Policy
  - –Used to configure settings for systems not part of AD

Account Restrictions

- Time of day restrictions
  - –Limits the time of day a user may log onto a system
  - –Time blocks for permitted access are chosen
  - –Can be set on individual systems
- Account expiration
  - –Orphaned accounts: accounts that remain active after an employee has left the organization
  - –Dormant accounts: not accessed for a lengthy period of time
  - –Both can be security risks

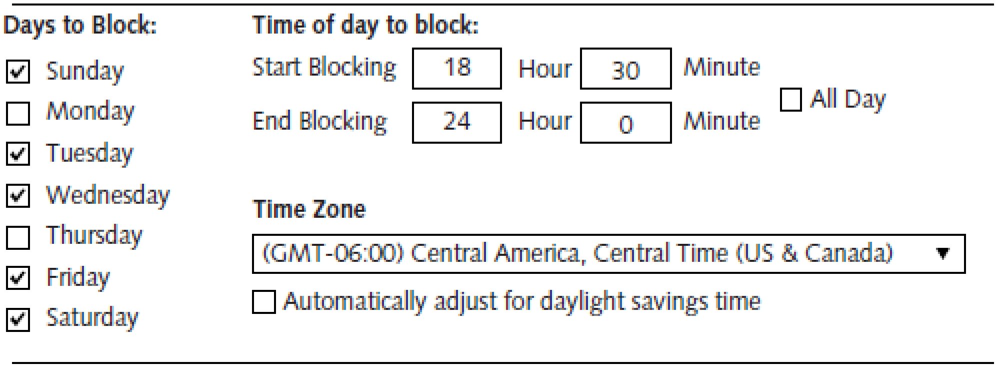
Recommendations for dealing with orphaned or dormant accounts

– Establish a formal process
– Terminate access immediately
– Monitor logs

Account expiration

– Sets a user's account to expire
– Password expiration sets a time when user must create a new password
–Different from account expiration
– Account expiration can be a set date, or a number of days of inactivity

Account Restrictions



Days to Block:

- ☑ Sunday
- □ Monday
- ☑ Tuesday
- ☑ Wednesday
- □ Thursday
- ☑ Friday
- ☑ Saturday

Time of day to block:

Start Blocking 18 Hour 30 Minute

End Blocking 24 Hour 0 Minute

□ All Day

Time Zone

(GMT-06:00) Central America, Central Time (US & Canada) ▼

□ Automatically adjust for daylight savings time

Figure 11-5 Time-of-day restrictions setting specific times and days

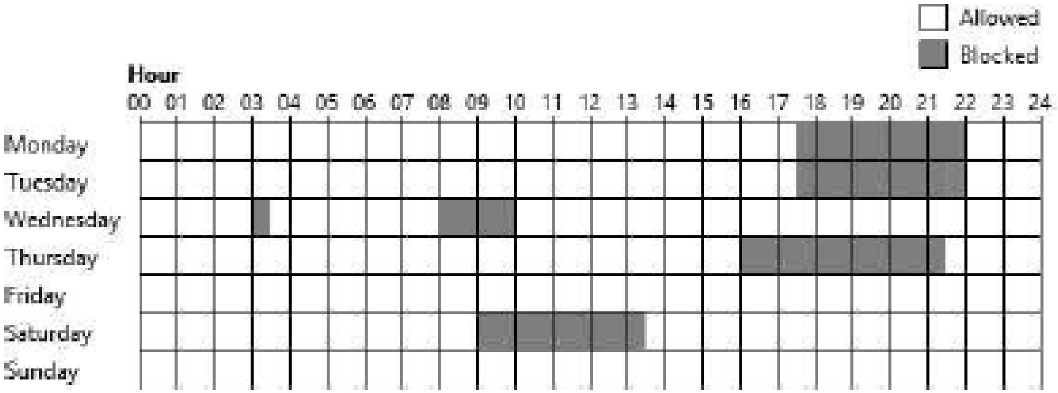


Figure 11-6 Time-of-day restrictions using a GUI

Operating system time of day restrictions

Authentication Services

- Process of verifying credentials
- Authentication services provided on a network
  - –Dedicated authentication server
    - •Or AAA server if it also performs authorization and accounting

- Common types of authentication and AAA servers

Kerberos

RADIUS

TACACS

LDAP

Authentication Services: Kerberos

- Authentication system developed at MIT
  - –Uses encryption and authentication for security
- Most often used in educational and government settings
- A network user requests access to services, Kerberos issues an identifying **ticket**, and the ticket is examined by the entity that grants access to the service.
- Kerberos ticket
  - –Contains information linking it to the user
  - –User presents ticket to network for a service
  - –Difficult to copy
  - –Expires after a few hours or a day

Authentication Services: TACACS

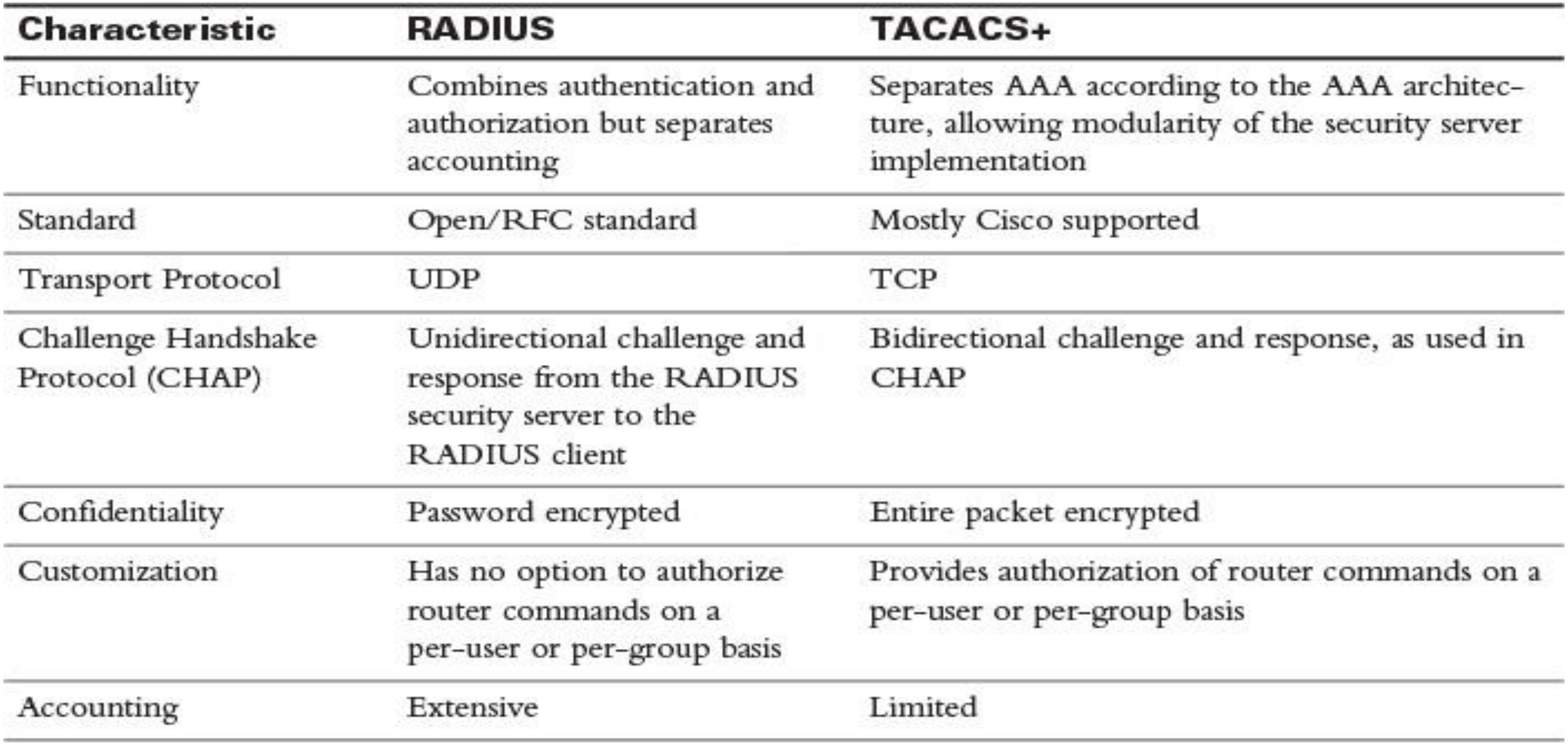
- Terminal Access Control Access Control System (TACACS)
  - Authentication service similar to RADIUS
  - Developed by Cisco Systems
  - It performs authentication, authorization, and accounting functions, and is meant to support a large number of connections.

Authentication Services: RADIUS

- Remote Authentication User Dial-In Service (RADIUS) has some specific and non-intuitive terminology.

  - supplicant - a wireless **device requesting to join** a WLAN, or a dial up device requesting to join a LAN
  - authenticator - an **access point** that **accepts or rejects** supplicants
  - RADIUS client - an **access point** that is **sending credentials** to a RADIUS server
  - RADIUS server -performs **authentication**, **authorization**, and **accounting** functions, and is meant to support a large number of connections.

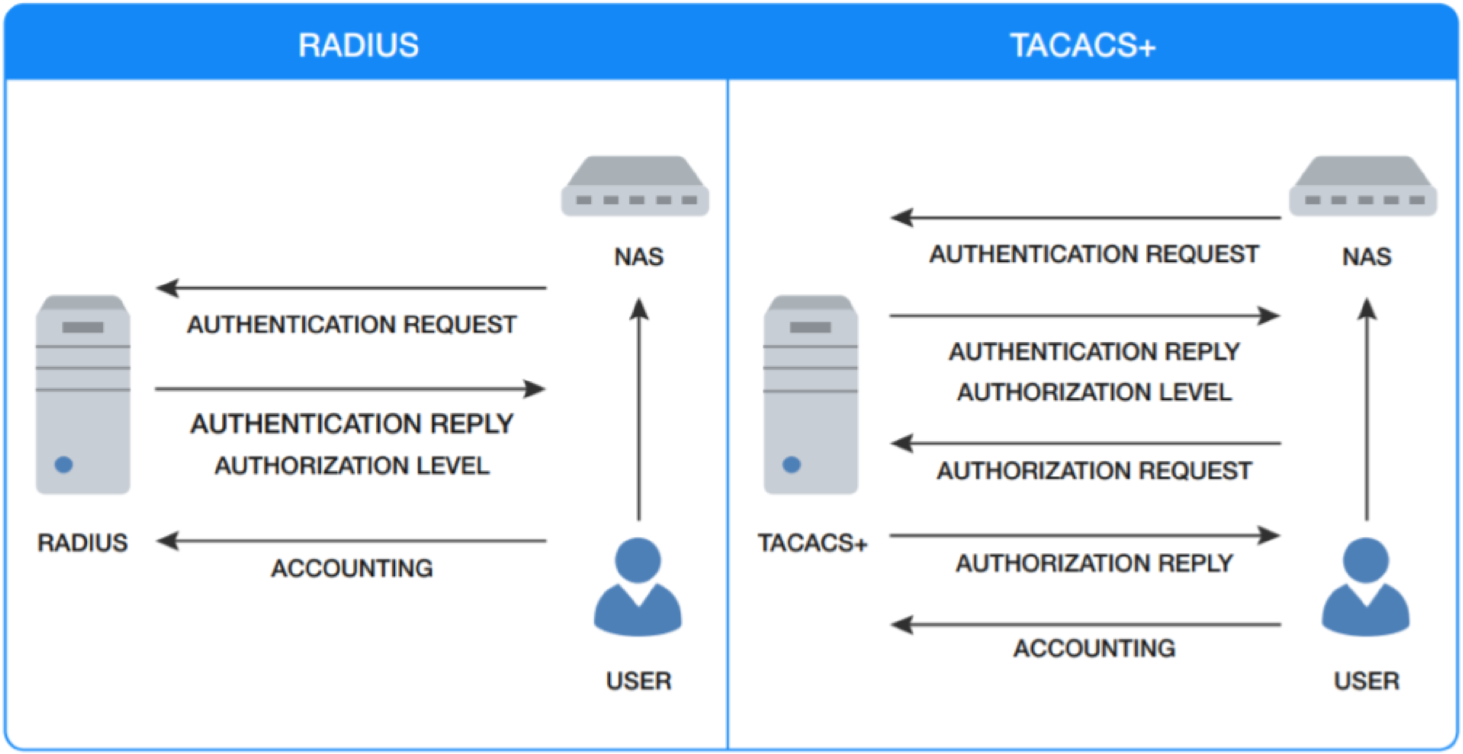
Authentication Services: RADIUS vs TACACS



Characteristic	RADIUS	TACACS+
Functionality	Combines authentication and authorization but separates accounting	Separates AAA according to the AAA architecture, allowing modularity of the security server implementation
Standard	Open/RFC standard	Mostly Cisco supported
Transport Protocol	UDP	TCP
Challenge Handshake Protocol (CHAP)	Unidirectional challenge and response from the RADIUS security server to the RADIUS client	Bidirectional challenge and response, as used in CHAP
Confidentiality	Password encrypted	Entire packet encrypted
Customization	Has no option to authorize router commands on a per-user or per-group basis	Provides authorization of router commands on a per-user or per-group basis
Accounting	Extensive	Limited

Comparison of RADIUS and TACACS+

Authentication Services: RADIUS vs TACACS



Comparison of RADIUS and TACACS+

Authentication Services: LDAP

- Lightweight Directory Access Protocol
- LDAP is a protocol that is used to access such databases.
- Directory service
  - –Database stored on a network
  - –Contains information about users and network devices
  - –Keeps track of network resources and user's privileges to those resources
  - –Grants or denies access based on its information

WEAKNESS

- Can be subject to LDAP injection attacks
  - -Similar to SQL injection attacks
  - -Occurs when user input is not properly filtered

Summary

- Access control is the process by which resources or services are denied or granted
- Four major access control models exist
- Best practices for implementing access control
  - –Separation of duties
  - –Job rotation
  - –Least privilege
  - –Mandatory vacations
- Access control lists define which subjects are allowed to access which objects
  - –Specify which operations they may perform
- Group Policy is a Windows feature that provides centralized management and configuration
- Authentication services can be provided on a network by a dedicated AAA or authentication server
  - –RADIUS is the industry standard