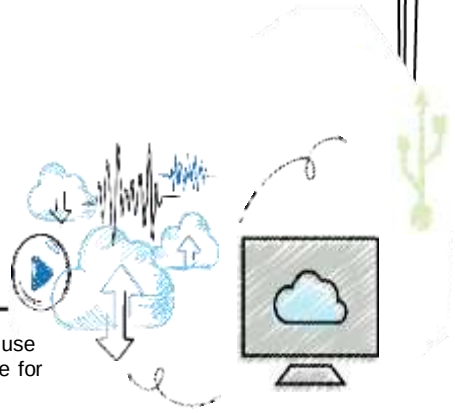
CompTIA Security+ Guide to Network Security Fundamentals, Sixth Edition

Chapter 12

Access Management



Objectives

12.1 Define access management and list the access control models

12.2 Describe how to manage access through account management

12.3 List the best practices for access control

12.4 Describe how to implement access control

12.5 Explain the different types of identity and access services

What is Access Control?

- Access Control
  - Granting or denying approval to use specific resources
- Physical access control
  - Consists of fencing, hardware door locks, and mantraps to limit contact with devices
- Technical access control
  - Consists of technology restrictions that limit users on computers from accessing data
- There are standard access control models that are used to help enforce access control

Access Control Terminology (1 of 5)

- Identification
  - Presenting credentials
  - Example: delivery driver presenting employee badge
- Authentication
  - Checking the credentials
  - Example: examining the delivery driver's badge
- Authorization
  - Granting permission to take action
  - Example: allowing delivery driver to pick up package
- Accounting
  - A record that is preserved of who accessed the network, what resources they accessed, and when they disconnected

Access Control Terminology (2 of 5)

Action	Description	Scenario example	Computer process
Identification	Review of credentials	Delivery person shows employee badge	User enters user name
Authentication	Validate credentials as genuine	Gabe reads badge to determine it is real	User provides password
Authorization	Permission granted for admittance	Gabe opens door to allow delivery person in	User authorized to log in
Access	Right given to access specific resources	Delivery person can only retrieve box by door	User allowed to access only specific data
Accounting	Record of user actions	Gabe signs to confirm the package was picked up	Information recorded in log file

Access Control Terminology (3 of 5)

- Object
  - A specific resource
  - Example: file or hardware device
- Subject
  - A user or process functioning on behalf of a user
  - Example: computer user
- Operation
  - The action taken by the subject over an object
  - Example: deleting a file

Access Control Terminology (4 of 5)

Role	Description	Duties	Example
Privacy officer	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
Custodian or 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
Owner	Person responsible for the information	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
End user	User who access information in the course of routine job responsibilities	Follows organization's security guidelines and does not attempt to circumvent security	Opens SALARY.XLSX

Access Control Terminology (5 of 5)

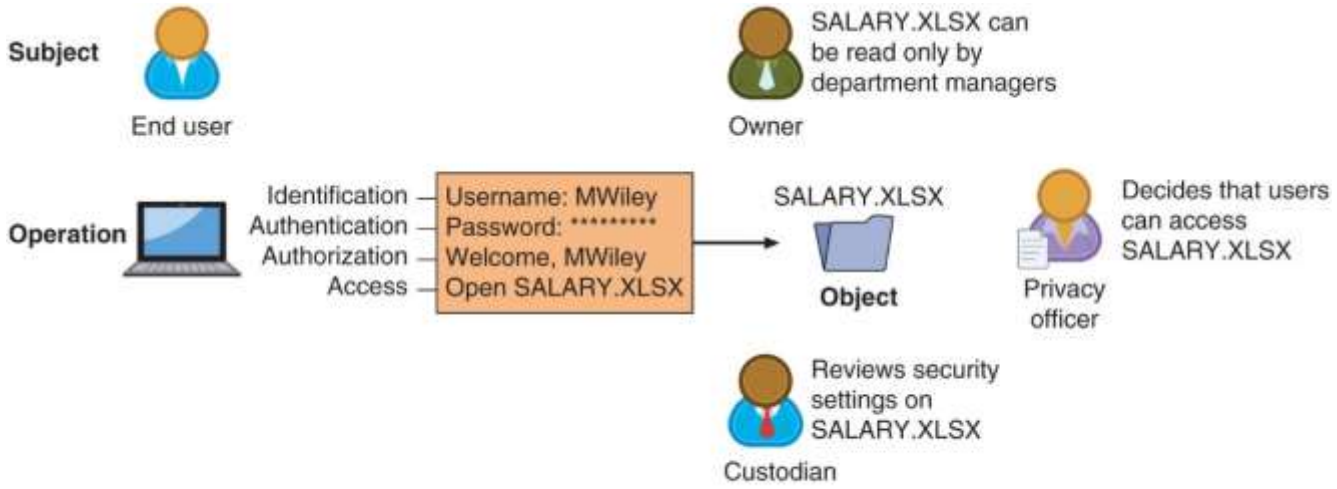


Figure 12-1 Technical access control process and terminology

Access Control Models

- Access control model
  - Standards that provide a predefined framework for hardware or software developers
  - Use the appropriate model to configure the necessary level of control
- Five major access control models
  - Discretionary Access Control (DAC)
  - Mandatory Access Control (MAC)
  - Role Based Access Control (RBAC)
  - Rule Based Access Control
  - Attribute-Based Access Control (ABAC)

Discretionary Access Control (DAC) (1 of 2)

- 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
- Used on operating systems such as most types of UNIX and Microsoft Windows
- Two significant weaknesses:
  - Poses a risk in that it relies on decision by the end user to set the proper level of security
  - A subject's permissions will be "inherited" by any programs that the subject executes

Discretionary Access Control (DAC) (2 of 2)

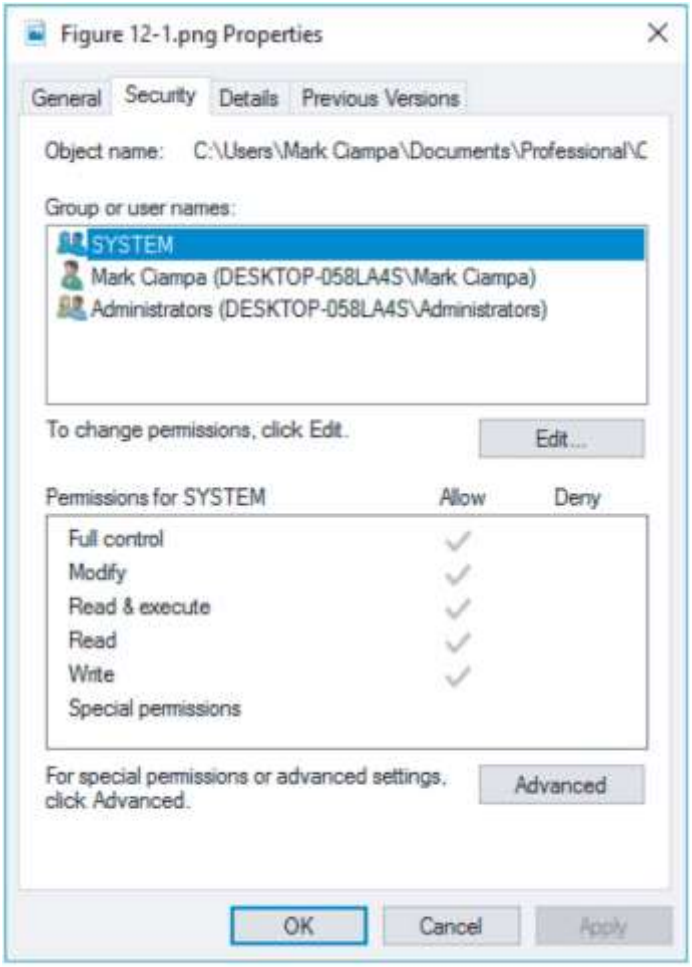


Figure 12-2 Windows Discretionary Access Control (DAC)

Mandatory Access Control (MAC) (1 of 4)

- Most restrictive access control model
  - User has no freedom to set any controls or distribute access to other subjects
- Typically found in military settings
- Two elements
  - Labels - Every entity is an object and is assigned a classification label that represents the relative importance of the object
    - Subjects are assigned a privilege label (clearance)
  - Levels - a hierarchy based on the labels is used
    - Top secret has a higher level than secret, which has a higher level than confidential
- MAC grants permissions by matching object labels with subject labels
  - Labels indicate level of privilege

Mandatory Access Control (MAC) (2 of 4)

- To determine if file may be opened:
  - Object and subject labels are compared
  - The subject must have equal or greater level than object to be granted access
- Two major implementations of MAC
  - Lattice model and Bell-LaPadula model
- Lattice model
  - Subjects and objects are assigned a “rung” on the lattice
  - Multiple lattices can be placed beside each other
- Bell-LaPadula (BLP) model
  - Similar to lattice model
  - Subjects may not create a new object or perform specific functions on lower level objects

Mandatory Access Control (MAC) (3 of 4)

- Microsoft Windows uses a MAC implementation called Mandatory Integrity Control (MIC)
  - A security identifier (SID) is issued to the user, group, or session
  - Each time a user logs in, the SID is retrieved from the database for that user
  - SID is used to identify user with subsequent interactions with Windows
  - Windows links the SID to an integrity level
  - User Access Control (UAC) - a Windows feature that controls user access to resources

Mandatory Access Control (MAC) (4 of 4)

Figure 12-3 Windows User Account Control (UAC) prompt

Role-Based Access Control

- 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

Rule-Based Access Control

- Also called Rule-Based Role-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

Attribute-Based Access Control (1 of 2)

- Uses more flexible polices than Rule-Based AC
  - Can combine attributes
- Policies can take advantage of attributes such as:
  - Object attributes
  - Subject attributes
  - Environment attributes
- ABAC rules can be formatted using an If-Then-Else structure

Attribute-Based Access Control (2 of 2)

Name	Explanation	Description
Mandatory Access Control (MAC)	End user cannot set controls	Most restrictive model
Discretionary Access Control (DAC)	Subject has total control over objects	Least restrictive model
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 model

Managing Access Through Account Management

- Properly configuring accounts is a first step in providing strong security
- Accounts include not only user accounts but also:
  - Service accounts
  - Privileged accounts
- Account management includes account setup as well as account auditing

Account Setup

- When initially setting up an account, take these into consideration:
  - Employee accounts
  - Creating location-based policies
  - Establishing standard naming conventions
  - Creating time-of-day restrictions
  - Enforcing least privilege

Employee Accounts (1 of 2)

- Employee Accounts are often the source of entry points by threat actors
- Employee Onboarding
  - Refers to the tasks associated with hiring a new employee
  - Onboarding steps:
    - Scheduling
    - Job duties
    - Socializing
    - Work space
    - Training
  - In addition, in a Microsoft Windows environment the steps may include:
    - Provision the new computer
    - Create email mailboxes and AD users
    - Add user accounts to groups
    - Create home folder
    - Review security settings

Employee Accounts (2 of 2)

- Employee offboarding
  - Actions to be taken when an employee leaves an enterprise
  - Steps include:
    - Back up all employee files from local computer and server
    - Archive email
    - Forward email to a manager or coworker
    - Hide the name from the email address book
  - Orphaned accounts – user accounts that remain active after an employee has left
  - Dormant account – an account that has not been accessed for a lengthy period
- Many organizations disable accounts for a minimum of 30 days and then purge disabled accounts twice per year

Location-Based Policies

- Geofencing relies upon location-based policies
  - Or establishing the geographical boundaries of where a mobile device can and cannot be used
- Polices are often first prescribed by generating an IP location data file
  - Which is a text file containing comma separated fields in the format IP_From, IP_To, Country_Code, Country_Name, Region, City
- This policy then becomes the basis for how authorization requests from mobile devices are evaluated

Standard Naming Conventions

- Standard naming conventions
  - “Rules” that have been established for creating account names
- Options typically include:
  - First initial of first name followed by last name,
  - First name with a punctuation mark followed by last name
  - Last name followed by department code
- In the event two names appear to be the same
  - A standard policy should be established for resolving conflicts

Time-of-Day Restrictions

- Time-of-day restrictions can be used to limit when a user can log into their account

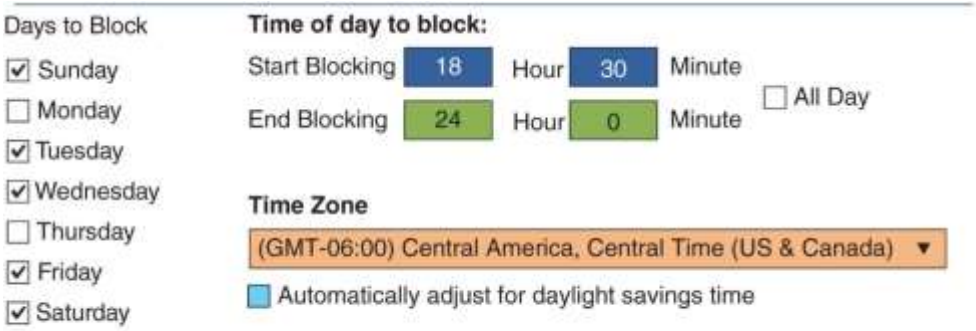


Figure 12-4 Time-of-day restrictions setting specific times and days

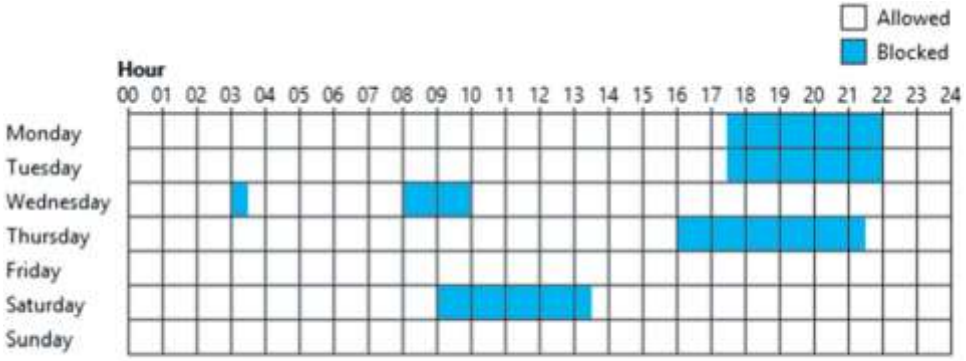


Figure 12-5 Time-of-day restrictions using GUI

Least Privilege

- Least privilege in access control
  - Means that only the minimum amount of privileges necessary to perform a job or function should be allocated
- Helps reduce the attack surface by eliminating unnecessary privileges that could provide an avenue for an attacker
- Should apply both to user accounts and to processes running on the system

Account Auditing

- Once accounts have been created, they should be periodically maintained and audited using the following audits:
  - Recertification – the process of periodically revalidating a user's account, access control, and membership role
  - Permission auditing and review – intended to examine the permissions that a user has been given to determine if each is still necessary
  - Usage auditing and review – an audit process that looks at the applications that the user is provided, how frequently they are used, and how they are being used

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
  - Mandatory vacations
  - Clean desk policy

Separation of Duties

- Separation of duties
  - Fraud can result from a single user being trusted with complete control of a process
  - Requires two or more people responsible for functions related to handling money
  - The system is not vulnerable to actions of a single person
- In relation to computer access control
  - Requires that if the fraudulent application of a process could potentially result in a breach of security, the process should be divided between two or more individuals

Job Rotation

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

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

Clean Desk Policy

- Designed to ensure that all confidential or sensitive materials are removed form a user's workspace and secured when the items not in use
  - Either in paper form or electronic
- Sample statements that might be found in a clean desk policy:
  - Computer workstations must be locked when the workspace is unoccupied and turned off at the end of the day
  - Confidential or sensitive information must be removed from the desk and locked in a drawer or safe when the desk is unoccupied or at the end of a work day
  - File cabinets must be kept closed and locked when not in use or not attended, and keys may not be left at an unattended desk
  - Laptops must be either locked with a locking cable or locked in a drawer or filing cabinet

Implementing Access Control

- Technologies used to implement access control:
  - Access control lists (ACLs)
  - Group-based access control

Access Control Lists (ACLs) (1 of 2)

- Access management ACL
  - A set of permissions attached to an object
- Specifies which subjects may access the object and what operations they can perform
- When a subject requests to perform an operation:
  - System checks ACL for an approved entry
- ACLs are usually viewed in relation to operating system files
- ACLs provide file system security for protecting files managed by the OS
- ACL have also been ported to SQL and relational database systems
  - So that ACLs can provide database security

Access Control Lists (ACLs) (2 of 2)

- Each entry in the ACL table is called access control entry (ACE)
- ACE structure (Windows)
  - Security identifier (SID) 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-Based Access Control

- Group-based access control
  - Permits the configuration of multiple computers by setting a single policy for enforcement
- One example of group-based access Control is Group Policy
  - A Microsoft Windows feature that 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 (LGP)
  - Has fewer options than a Group Policy
  - Used to configure settings for systems not part of AD

Identity and Access Services

- Different services can be used to provide identity and access services:
  - RADIUS
  - Kerberos
  - Terminal Access Control Access Control Systems
  - Generic servers built on the Lightweight Directory Access Protocol (LDAP)
  - Security Assertion Markup Language
  - Authentication framework protocols

RADIUS (1 of 2)

- Remote Authentication Dial In User Service
  - Developed in 1992
  - Became an industry standard
  - Originally designed for remote dial-in access to a corporate network
- RADIUS client
  - Typically a device such as a wireless AP
    - Responsible for sending user credentials and connection parameters to the RADIUS server
- RADIUS user profiles are stored in a central database that all remote servers can share
- Advantages of a central service
  - Increases security due to a single administered network point
  - Easier to track usage for billing and keeping network statistics

RADIUS (2 of 2)

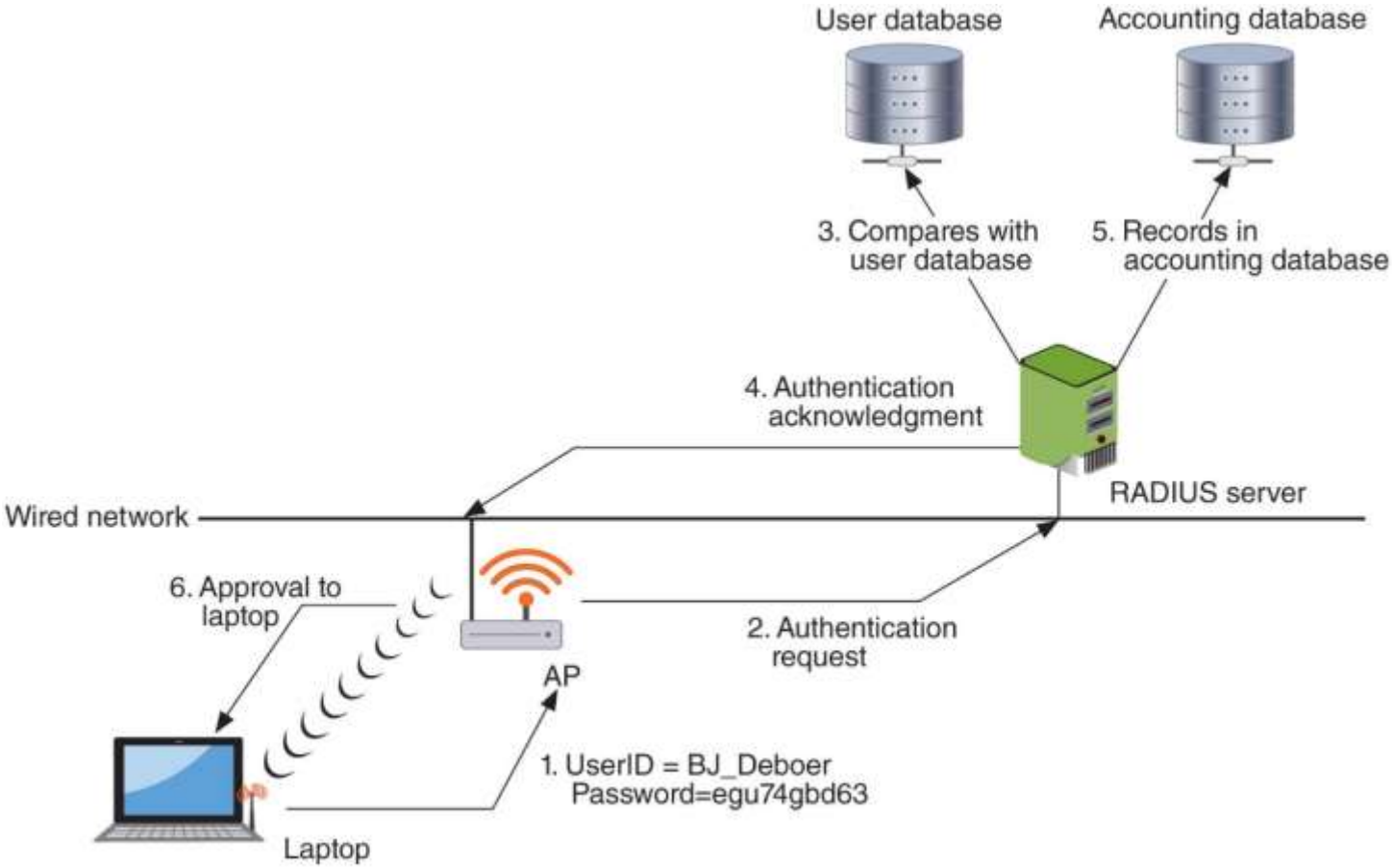


Figure 12-6 RADIUS authentication

Kerberos

- Authentication system developed at MIT
  - Uses encryption and authentication for security
- Works like using a driver's license to cash a check
- Kerberos ticket characteristics:
  - Difficult to copy
  - Contains information linking it to the user
  - It lists restrictions
  - Expires at some future date

Terminal Access Control Access Control System+ (TACACS+) (1 of 2)

- Authentication service similar to RADIUS
- Commonly used on UNIX devices
- Communicates by forwarding user authentication information to a centralized server
- The current version is TACACS+

Terminal Access Control Access Control System+ (TACACS+) (2 of 2)

Feature	RADIUS	TACACS+
Transport Protocol	User Datagram Protocol (UDP)	Transmission Control Protocol (TCP)
Authentication and authorization	Combined	Separate
Communication	Unencrypted	Encrypted
Interacts with Kerberos	No	Yes
Can authenticate network devices	No	Yes

Lightweight Directory Access Protocol (LDAP) (1 of 2)

- A directory service is a 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
- Standard for directory services is known as X.500
  - Purpose of the standard was to standardize how the data was stored so that any computer system could access directories
- X.500 standard also defines a protocol for client application to access the DAP
  - LDAP

Lightweight Directory Access Protocol (LDAP) (2 of 2)

- LDAP
  - Designed to run over TCP/IP
  - A simpler subset of DAP
  - Encodes protocol elements in simpler way than X.500
- LDAP traffic is transmitted in cleartext
  - Can be made secure by using SSL or TLS
  - Known as Secure LDAP or LDAP over SSL (LDAPS)
- Weakness of LDAP
  - Can be subject to LDAP injection attacks
    - Similar to SQL injection attacks
    - Occurs when user input is not properly filtered

Security Assertion Markup Language (SAML) (1 of 2)

- SAML
  - An Extensible Markup Language (XML) standard that allows secure web domains to exchange user authentication and authorization data
  - Allows a user's login credentials to be stored with a single identity provider instead of being stored on each web service provider's server
  - Used extensively for online e-commerce business-to-business (B2B) and business-to-customer (B2C) transactions

Security Assertion Markup Language (SAML) (2 of 2)

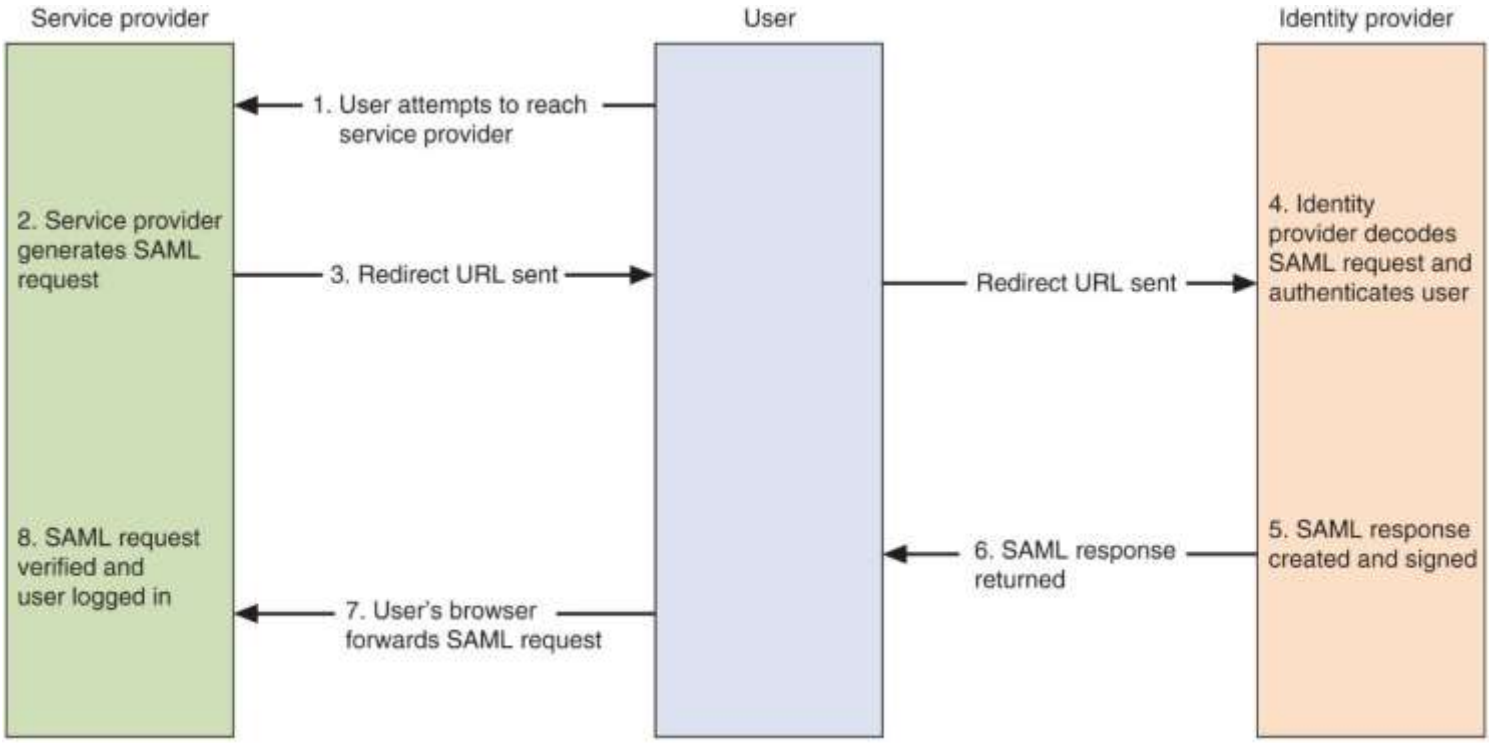


Figure 12-7 SAML transaction

Authentication Framework Protocols

- A framework for transporting authentication protocols is known as the Extensible Authentication Protocol (EAP)
- EAP was created as a more secure alternative to:
  - Challenge-Handshake Authentication Protocol (CHAP)
  - The Microsoft version of CHAP (MS-CHAP)
  - Password Authentication Protocol (PAP)
- EAP:
  - Defines the format of the messages
  - Uses four types of packets:
    - Request, response, success, and failure

Chapter Summary (1 of 2)

- Access control is the process by which resources or services are denied or granted
- Five major access control models:
  - Discretionary Access Control, Mandatory Access Control, Role-Based Access Control, Rule-Based Access Control, Attribute-Based Access Control
- Configuring accounts with proper permissions is the first step in providing strong security
- Location-based policies establish the geographical boundaries of where a mobile device can and cannot be used
- Once accounts have been created, it is important that they be periodically maintained and audited to ensure they still follow all enterprise policies

Chapter Summary (2 of 2)

- Best practices for implementing access control
  - Separation of duties, job rotation, mandatory vacations, and following a clean desk policy
- Implementing access control methods includes using access control lists (ACLs)
- Different services can be used to provide identity and access services
- A directory service is a database stored on the network itself that contains information about users and network devices
- One implementation of a directory service as an authentication is the Lightweight Directory Access Protocol (LDAP)