

Information Security (CP3404)

Chapter 11 – Access Control Fundamentals

Based on the Fifth Edition of:

M. Ciampa: *CompTIA® Security + Guide to Network Security Fundamentals*

Department of Information Technology, College of Business, Law & Governance



Learning Objectives



- Define access control and list the four access control models
- Describe how to implement access control
- Explain the different types of authentication services

Outline

- 1 What is Access Control
- 2 Implementing Access Control
- 3 Authentication Services

Preface



- Users first must be identified as authorized user, such as by logging in with user name and password to laptop computer
- Because laptop connects to corporate network that contains critical data, important also to restrict user access to only software, hardware, and other resources for which user has been approved
- These two acts —**authenticating only approved users** and **controlling their access to resources**— are important foundations in information security




What is Access Control?

- **Access control** – Granting or denying approval to use specific resources; it is controlling access
- **Physical access control** – Fencing, hardware door locks, and mantraps that limit contact with devices
- **Technical access control** – Technology restrictions that limit users on computers from accessing data
- Access control has set of associated terminology to describe actions
- There are **four (4)** standard access control models as well as specific practices used to enforce access control

What is Access Control?

Access Control Terminology

- **Identification**  Presenting credentials (Example: delivery driver presenting employee badge)
- **Authentication** – Checking credentials (Example: examining the delivery driver's badge)
- **Authorization** – Granting permission to take action (Example: allowing delivery driver to pick up package) – see Table 11-1

What is Access Control?

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

Table 11-1 Basic steps in access control

What is Access Control?

Access Control Terminology (Cont.)

- **Object** – Specific resource (Example: file or hardware device)
- **Subject** – User or process functioning on behalf of a user (Example: computer user)
- **Operation** – Action taken by the subject over an object (Example: deleting file)
- Individuals are given different roles in relationship to access control objects or resources (see Table 11-2)
- Figure 11-1 illustrates the technical access control process and terminology

What is Access Control?

Role	Description	Duties	Example
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
Custodian	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
End-user	User who accesses information in the course of routine job responsibilities	Follows organization's security guidelines and does not attempt to circumvent security	Opens SALARY.XLSX

Table 11-2 Roles in access control

What is Access Control?

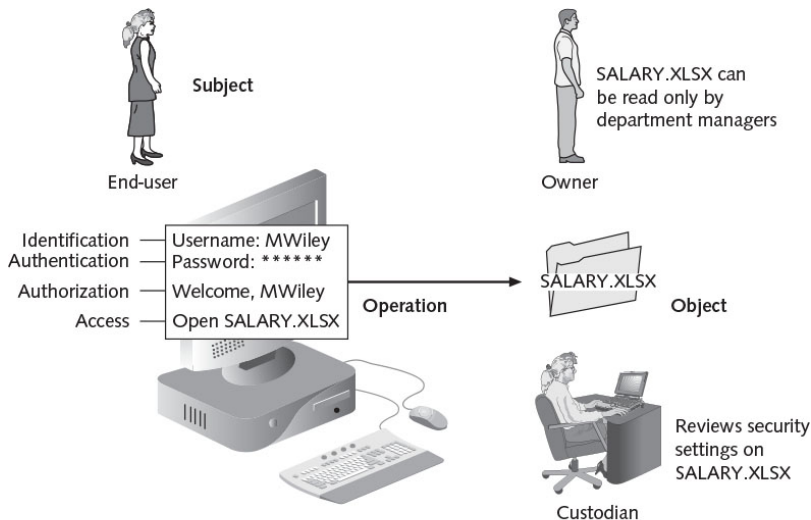


Figure 11-1 Technical access control process and terminology

What is Access Control?

Access Control Models

- **Access control model** – Hardware and software predefined framework that custodian can use for controlling access
- Access control models used by custodians for access control are neither created nor installed by custodians or users; instead, these models are already part of software and hardware.
- **Four (4)** major access control models:
 - ① **Discretionary Access Control (DAC)**
 - ② **Mandatory Access Control (MAC)**
 - ③ **Role Based Access Control (RBAC)**
 - ④ **Rule based Access Control (RBAC)**

What is Access Control?

Discretionary Access Control (DAC)

- Discretionary Access Control (DAC) – Least restrictive model
- Every object has owner, who has total control over that object
- Owners can create and access their objects freely
- Owner can give permissions to other subjects over these objects
- DAC used on operating systems like UNIX and Microsoft Windows (see Figure 11-2)

What is Access Control?

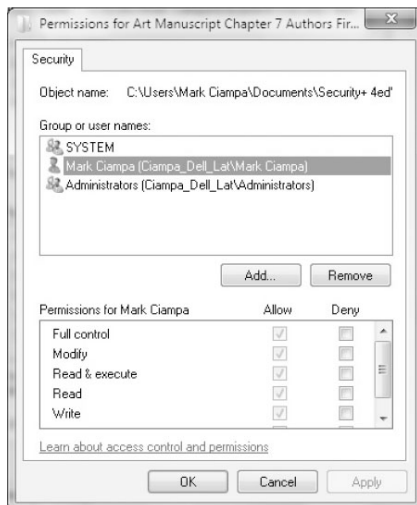


Figure 11-2 Windows Discretionary Access Control (DAC)

Source: Microsoft Windows

What is Access Control?



Discretionary Access Control (DAC) — Weaknesses

- DAC has **two (2)** significant weaknesses:
 - ① DAC relies on decisions by end-user to set proper level of security; incorrect permissions might be granted to subject or permissions might be given to unauthorized subject
 - ② Subject's permissions will be *inherited* by any programs that subject executes; attackers often take advantage of this inheritance because end-users frequently have a high level of privileges

What is Access Control?

Mandatory Access Control (MAC)

- **Mandatory Access Control (MAC)** – Opposite of DAC and is most restrictive access control model
- MAC assigns users access controls strictly according to custodian's desires and user has no freedom to set any controls

What is Access Control?

Mandatory Access Control (MAC)

- Two (2) key elements to MAC:
 - 1 **Labels** – Every entity is an object (laptops, files, projects, and so on) and assigned classification label (confidential, secret, and top secret) while subjects assigned privilege label (a clearance)
 - 2 **Levels** – Hierarchy based on labels is also used, both for objects and subjects (Top secret higher level than secret)
- MAC grants permissions by matching object labels with subject labels based on their respective levels

What is Access Control?

Mandatory Access Control (MAC) — Implementation

- A **Security Identifier (SID)** is a unique number issued to the user, group, or session
- Each time the user logs in, the system retrieves the SID for that user from the database
- Windows links the SID to an **integrity level**
- this is done through **User Account Control (UAC)** that attempts to match the subject's privilege level with that of the object (see Figure 11-3)

What is Access Control?

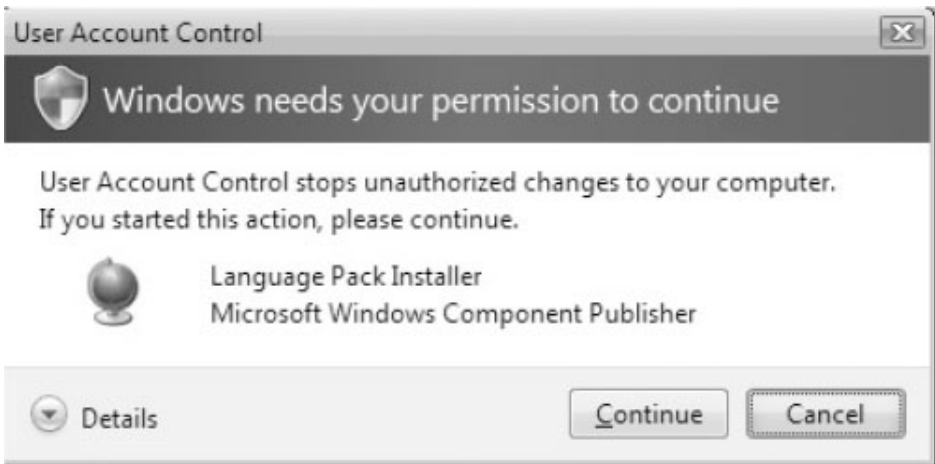


Figure 11-3 Windows User Account Control (UAC) prompt

Source: Microsoft Windows

What is Access Control?



Role Based Access Control (RBAC)

- **Role Based Access Control (RBAC)** – Considered more *real-world* access control than other models because access based on user's job function within organization
- Instead of setting permissions for each user or group assigns permissions to particular roles in organization and then assigns users to those roles
- Objects are set to be a certain type, to which subjects with that particular role have access

What is Access Control?

Rule Based Access Control (RBAC)

- **Rule Based Access Control (RBAC)** – Dynamically assign roles to subjects based on set of rules defined by custodian
- Each resource object contains set of access properties based on rules
- When user attempts to access that resource, system checks rules contained in object to determine if access is permissible

Table 11-3 summarizes the features of the **four (4)** access Control models

What is Access Control?

Name	Restrictions	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 (RBAC)	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

Table 11-3 Access control models

What is Access Control?

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

What is Access Control?



Best Practices for Access Control — Separation of Duties

- Separation of duties – Not to give one person total control
- 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

What is Access Control?

Best Practices for Access Control — Job Rotation

- **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 position to manipulate security configurations
 - Helps expose potential avenues for fraud
 - Reduces employee burnout

What is Access Control?

Best Practices for Access Control — Least Privilege

- **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 due to the challenges of assigning users lower security levels (see Table 11-4)

What is Access Control?

Challenge	Explanation
Legacy applications	Many older software applications were designed to run only 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. Redesigning 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.

Table 11-4 Challenges of least privilege

What is Access Control?

Best Practices for Access Control — Implicit Deny

- **Implicit deny** – If condition is not explicitly met, access request is rejected
- *Example:* Network router rejects access to all except conditions matching the rule restrictions
- When creating access control restrictions, recommended that unless condition is specifically met then access should be denied

What is Access Control?



Best Practices for Access Control — Mandatory Vacations

- **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

Implementing Access Control



Implementing Access Control

- Several technologies can be used to implement access control:
 - Access Control Lists (ACLs)
 - Group Policies
 - Account Restrictions

Implementing Access Control



Access Control Lists (ACLs)

- **Access control list (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 (see Figure 11-4)

Implementing Access Control



```
$ setfacl -m user:tdk:rw- samplefile
$ getacl samplefile
# file: samplefile
# owner: reo
# group: sysadmin
user::rw-user:
tdk:rw-                #effective:r--
group::r--              #effective:r--
mask:r--
other:r--
```

Figure 11-4 UNIX file permissions

Implementing Access Control



Access Control Lists (ACLs) — Structure

- 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

Implementing Access Control



Access Control Lists (ACLs) — Limitations

- Although widely used, ACLs have limitations:
 - Using ACLs is not efficient – ACL for each file, process, or resource must be checked every time the resource is accessed.
 - Can be difficult to manage in an enterprise setting where many users need to have different levels of access to many different resources; selectively adding, deleting, and changing ACLs on individual files, or even groups of files, can be time-consuming and open to errors, particularly if changes must be made frequently

Implementing Access Control



Group Policies

- **Group Policy** – 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 and used to configure settings for systems not part of AD

Implementing Access Control



Account Restrictions

- Another means of enforcing access control is to place restrictions on user accounts
- Two (2) common account restrictions are:
 - 1 Time-of-Day Restrictions
 - 2 Account Expiration

Implementing Access Control



Account Restrictions — Time-of-Day Restrictions

- **Time of day restrictions** – Limits the time of day a user may log onto a system
- Time blocks for permitted access are chosen (see Figures 11-5 and 11-6)
- Can be set on individual systems

Implementing Access Control



Days to Block:

- ☒ Sunday
- ☐ Monday
- ☒ Tuesday
- ☒ Wednesday
- ☐ Thursday
- ☒ Friday
- ☒ Saturday

Time of day to block:

Start Blocking Hour Minute
End Blocking Hour Minute ☐ All Day

Time Zone

▼

☐ Automatically adjust for daylight savings time

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

Implementing Access Control

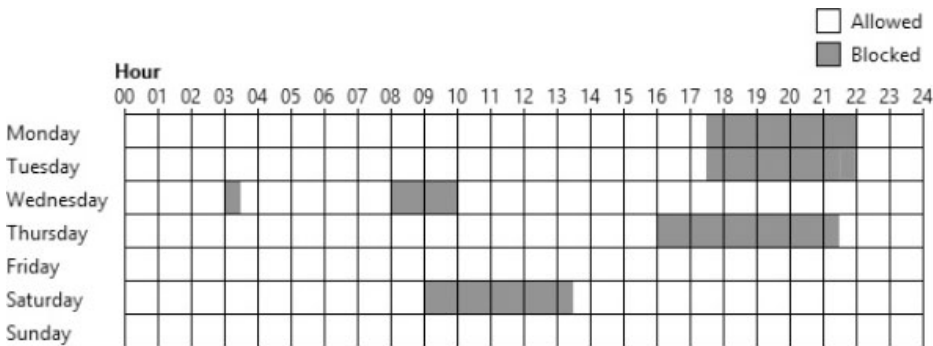


Figure 11-6 Time-of-day restrictions using a GUI

Source: Microsoft Windows

Implementing Access Control



Account Restrictions — Account Expiration

- **Orphaned accounts** – Accounts that remain active after employee has left organization
- **Dormant accounts** – Accounts not accessed for lengthy period of time
- Both can be security risks
- **Account expiration** – Process of setting a user's account to expire
- Account expiration can be explicit (account expires on a set date) or based on specific number of days of inactivity

Quick Quiz



- ① _____ is the process by which resources or services are granted or denied on a computer system or network.

Answer:

Quick Quiz



- ① _____ is the process by which resources or services are granted or denied on a computer system or network.

Answer: Access control

Quick Quiz



- ① _____ is the process by which resources or services are granted or denied on a computer system or network.

Answer: Access control

- ② A(n) _____ is a set of permissions that is attached to an object.

Answer:

Quick Quiz



- ① _____ is the process by which resources or services are granted or denied on a computer system or network.

Answer: Access control

- ② A(n) _____ is a set of permissions that is attached to an object.

Answer: access control list (ACL)

Quick Quiz



- ① _____ is the process by which resources or services are granted or denied on a computer system or network.

Answer: Access control

- ② A(n) _____ is a set of permissions that is attached to an object.

Answer: access control list (ACL)

- ③ _____ are user accounts that remain active after an employee has left an organization.

Answer:

Quick Quiz



- ① _____ is the process by which resources or services are granted or denied on a computer system or network.

Answer: Access control

- ② A(n) _____ is a set of permissions that is attached to an object.

Answer: access control list (ACL)

- ③ _____ are user accounts that remain active after an employee has left an organization.

Answer: Orphaned accounts

Quick Quiz



- ① _____ is the process by which resources or services are granted or denied on a computer system or network.

Answer: Access control

- ② A(n) _____ is a set of permissions that is attached to an object.

Answer: access control list (ACL)

- ③ _____ are user accounts that remain active after an employee has left an organization.

Answer: Orphaned accounts

- ④ Mandatory Integrity Control (MIC) uses a unique number issued to the user, group, or session called the _____.

Answer:

Quick Quiz



- ① _____ is the process by which resources or services are granted or denied on a computer system or network.

Answer: Access control

- ② A(n) _____ is a set of permissions that is attached to an object.

Answer: access control list (ACL)

- ③ _____ are user accounts that remain active after an employee has left an organization.

Answer: Orphaned accounts

- ④ Mandatory Integrity Control (MIC) uses a unique number issued to the user, group, or session called the _____.

Answer: Security identifier (SID)

Authentication Services



Authentication Services

- **Authentication** – Process of verifying credentials
- Authentication services can be provided on a network by a dedicated **Authentication, Authorization, and Accounting (AAA)** server, or by an **Authentication Server**.
- Common types of authentication and AAA servers:
 - **RADIUS**
 - **Kerberos**
 - **Terminal Access Control Access Control System (TACACS)**
 - **Lightweight Directory Access Protocol (LDAP)**
 - **Security Assertion Markup Language (SAML)**

Authentication Services



RADIUS (Remote Authentication Dial In User Service)

- **RADIUS** – Developed in 1992 and quickly became industry standard
- Originally designed for remote dial-in access to corporate network
- Remote in name almost misnomer: RADIUS authentication used for more than connecting to remote networks
- With development of IEEE 802.1x port security for both wired and wireless LANs, RADIUS seen even greater usage

Authentication Services



RADIUS (Remote Authentication Dial In User Service)

- RADIUS client is not device requesting authentication
- RADIUS client is device like wireless AP or dial-up server responsible for sending user credentials and connection parameters in form of RADIUS message to RADIUS server
- RADIUS server authenticates and authorizes RADIUS client request and sends back RADIUS message response
- RADIUS clients also send RADIUS accounting messages to RADIUS servers (see Figure 11-7)

Authentication Services

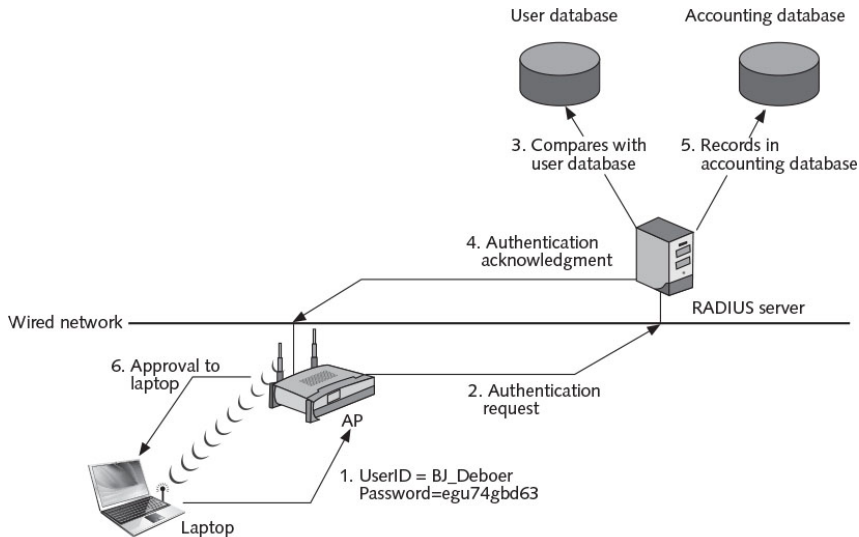


Figure 11-7 RADIUS authentication

Authentication Services



Kerberos

- **Kerberos** – Authentication system developed at MIT that uses encryption and authentication for security
- Most often used in educational and government settings
- 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



Terminal Access Control Access Control System (TACACS)

- **TACACS** – Authentication service commonly used on UNIX devices (similar to RADIUS)
- Communicates by forwarding user authentication information to a centralized server
- **Extended TACACS (XTACACS)** – Later version introduced in 1990
- The current version is **TACACS+**

Table 11-5 summarizes differences between TACACS+ and RADIUS

Authentication Services



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

Table 11-5 Comparison of RADIUS and TACACS+

Authentication Services



Lightweight Directory Access Protocol (LDAP)

- **Directory service** – Is a database stored on a network that 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
- **X.500** – Standard for directory services
- X.500 defines protocol for client application access called **Directory Access Protocol (DAP)**

Authentication Services



Lightweight Directory Access Protocol (LDAP)

- DAP is too large to run on a personal computer.
- **LDAP** – Simpler subset of DAP
 - Designed to run over TCP/IP
 - Has simpler functions
 - Encodes protocol elements simpler way than X.500
- **Secure LDAP** – LDAP over SSL (LDAPS)
- **LDAP injection attacks** – Attacks when user input not properly filtered

Authentication Services



Security Assertion Markup Language (SAML)

- **SAML** – Is an **Extensible Markup Language (XML)** standard that allows secure web domains exchange user authentication and authorization data
- Allows user's login credentials be stored with single identity provider instead of being stored on each web service provider's server
- SAML is used extensively for online e-commerce business-to-business (B2B) and business-to-consumer (B2C) transactions (see Figure 11-8)

Authentication Services

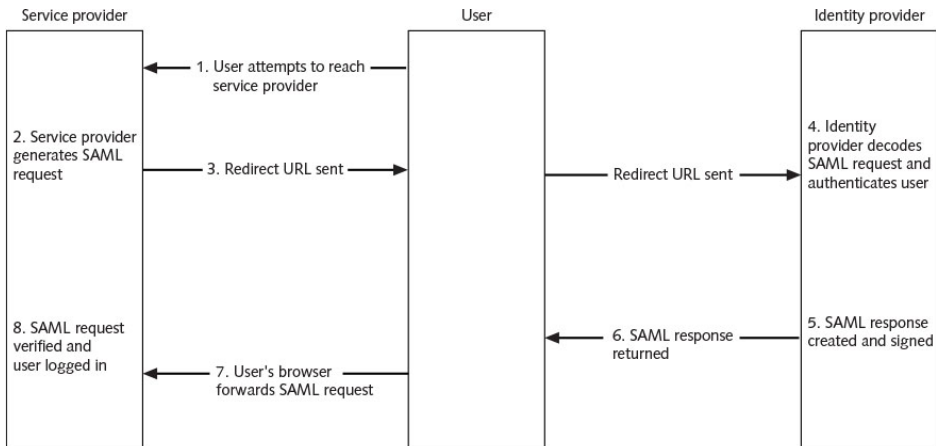


Figure 11-8 SAML transaction

Quick Quiz



- ① **True or False:** A RADIUS client is the device requesting authentication, such as a desktop system or wireless notebook computer.

Answer:

Quick Quiz



- ① **True or False:** A RADIUS client is the device requesting authentication, such as a desktop system or wireless notebook computer.

Answer: False

Quick Quiz



- ① **True or False:** A RADIUS client is the device requesting authentication, such as a desktop system or wireless notebook computer.

Answer: False

- ② _____ is an authentication system developed by the Massachusetts Institute of Technology (MIT) and used to verify the identity of networked users.

Answer:

Quick Quiz



- ① **True or False:** A RADIUS client is the device requesting authentication, such as a desktop system or wireless notebook computer.

Answer: False

- ② _____ is an authentication system developed by the Massachusetts Institute of Technology (MIT) and used to verify the identity of networked users.

Answer: Kerberos

Quick Quiz



- ❶ **True or False:** A RADIUS client is the device requesting authentication, such as a desktop system or wireless notebook computer.

Answer: False

- ❷ _____ is an authentication system developed by the Massachusetts Institute of Technology (MIT) and used to verify the identity of networked users.

Answer: Kerberos

- ❸ **True or False:** LDAP makes it possible for almost any application running on virtually any computer platform to obtain directory information.

Answer:

Quick Quiz



- ❶ **True or False:** A RADIUS client is the device requesting authentication, such as a desktop system or wireless notebook computer.

Answer: False

- ❷ _____ is an authentication system developed by the Massachusetts Institute of Technology (MIT) and used to verify the identity of networked users.

Answer: Kerberos

- ❸ **True or False:** LDAP makes it possible for almost any application running on virtually any computer platform to obtain directory information.

Answer: True