Welcome to the (ISC)^2 Certified Information Systems Security Professional (CISSP) Training Course

(ISC)^2®

CISSP®

Certified Information
Systems Security Professional

Domain 5

Identity and Access Management (IAM)

Domain Objectives

1. Identify standard terms for applying physical and logical access controls to environments related to their security practice.
2. Apply physical and logical access controls to environments with relation to the (environment’s or access controls’) security practice.
3. Define the process of user and systems access review.
4. Apply the appropriate control types/categories for provisioning and deprovisioning of identities.
5. Classify various identification, authentication, and authorization technologies and for use in managing people, devices, and services.

Domain Objectives (continued)

6. Differentiate the languages and protocols that are related to roles and systems that support federation.
7. Select the appropriate technologies and protocols for establishing a federated environment that satisfies business requirements.
8. Appraise various access control models to meet business security requirements.
9. Name the significance of accountability in relationship to identification, authentication, and auditing.

Domain Agenda

- Control Physical and Logical Access to Assets
- Identity and Access Provisioning Lifecycle
- Identification and Authentication of People, Devices, and Services
- Identity Management Implementation
- Implement and Manage Authorization Mechanisms

Domain Agenda (continued)

Accountability

Domain Review

Module 1

Control Physical and Logical Access to Assets

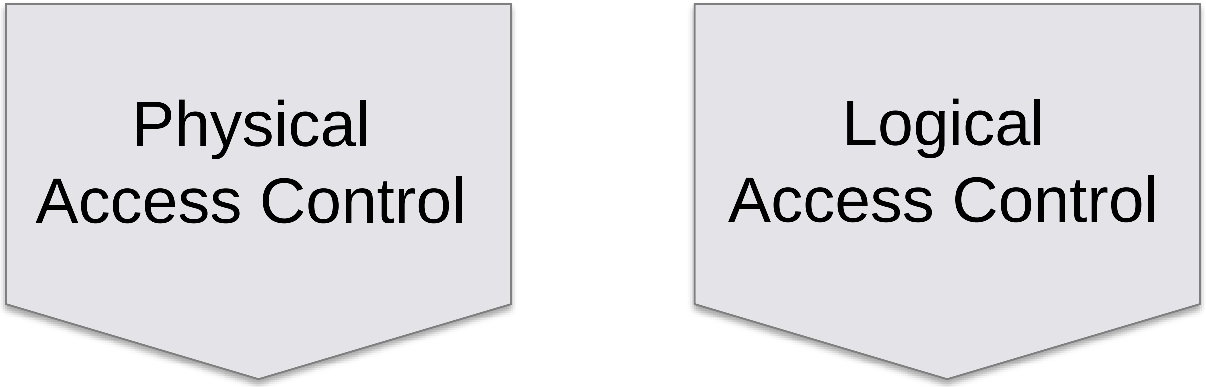
Module Objectives

1. Identify standard terms for applying physical and logical access controls to environments related to their security practice.
2. Apply physical and logical access controls to environments with relation to the (environment’s or access controls’) security practice.

Systems

- **Access control:** Authorization and restriction of access as specified by business and security requirements.
- **Logical access control system:** Automated system, controlling an individual’s ability to access computer systems.
- **Physical access control system:** Automated system that maintains passage of people or assets through a controlled opening.

Logical and Physical Access Control Systems



Physical Access Control

Logical Access Control

E.g., Mantrap

E.g., Client/Server login access

Devices

- Hardware/software
- Access control tokens
- Biometric readers

INFORMATION

SYSTEMS

DEVICES

FACILITIES

PERSONNEL

Comparing Subjects and Objects

Subject A *subject* is an active entity that accesses a passive object to receive information from, or data about, an object. Subjects can be users, programs, processes, services, computers, or anything else that can access a resource. When authorized, subjects can modify objects.

Object An *object* is a passive entity that provides information to active subjects. Some examples of objects include files, databases, computers, programs, processes, services, printers, and storage media.

Access is the flow of information between a subject and an object.

Types of Access Control

Types of Access Control

Generally, an access control is any hardware, software, or administrative policy or procedure that controls access to resources. The goal is to provide access to authorized subjects and prevent unauthorized access attempts. Access control includes the following overall steps:

1. Identify and authenticate users or other subjects attempting to access resources.
2. Determine whether the access is authorized.
3. Grant or restrict access based on the subject’s identity.
4. Monitor and record access attempts.
5. **Preventive Access Control** A *preventive control* attempts to thwart or stop unwanted or unauthorized activity from occurring.
6. **Detective Access Control** A *detective control* attempts to discover or detect unwanted or unauthorized activity.
7. **Corrective Access Control** A *corrective control* modifies the environment to return systems to normal after an unwanted or unauthorized activity has occurred.
8. **Deterrent Access Control** A *deterrent access control* attempts to discourage security policy violations.
9. **Recovery Access Control** A *recovery access control* attempts to repair or restore resources, functions, and capabilities after a security policy violation.

Administrative Access Controls *Administrative access controls* are the policies and procedures defined by an organization's security policy and other regulations or requirements.
Logical/Technical Controls *Logical access controls* (also known as *technical access controls*) are the hardware or software mechanisms used to manage access and to provide protection for resources and systems.
Physical Controls *Physical access controls* are items you can physically touch. They include physical mechanisms deployed to prevent, monitor, or detect direct contact with systems or areas within a facility.

Comparing Identification and Authentication
Identification is the process of a subject claiming, or professing, an identity. A subject must provide an identity to a system to start the authentication, authorization, and accountability processes.
Authentication verifies the identity of the subject by comparing one or more factors against a database of valid identities, such as user accounts.

Administrative Access Controls *Administrative access controls* are the policies and procedures defined by an organization’s security policy and other regulations or requirements.

Logical/Technical Controls *Logical access controls* (also known as *technical access controls*) are the hardware or software mechanisms used to manage access and to provide protection for resources and systems.

Physical Controls *Physical access controls* are items you can physically touch. They include physical mechanisms deployed to prevent, monitor, or detect direct contact with systems or areas within a facility.

Comparing Identification and Authentication

Identification is the process of a subject claiming, or professing, an identity. A subject must provide an identity to a system to start the authentication, authorization, and accountability processes.

Authentication verifies the identity of the subject by comparing one or more factors against a database of valid identities, such as user accounts.

Authorization and Accountability

Authorization Subjects are granted access to objects based on proven identities. For example, administrators grant users access to files based on the user’s proven identity.

Accountability Users and other subjects can be held accountable for their actions when auditing is implemented.

Authentication Factors

The three basic methods of authentication are also known as types or factors. They are as follows:

Type 1 A *Type 1 authentication factor* is something you know. Examples include a password, personal identification number (PIN), or passphrase.

Type 2 A *Type 2 authentication factor* is something you have. Physical devices that a user possesses can help them provide authentication. Examples include a smartcard, hardware token, *memory card*, or Universal Serial Bus (USB) drive.

Type 3 A *Type 3 authentication factor* is something you are or something you do. It is a physical characteristic of a person identified with different types of biometrics.

Somewhere You Are The somewhere-you-are factor identifies a subject's location based on a specific computer, a geographic location identified by an Internet Protocol (IP) address, or a phone number identified by caller ID.

Context-Aware Authentication Many mobile device management (MDM) systems use context-aware authentication to identify mobile device users.

Cognitive Passwords

Another password mechanism is the *cognitive password*. A cognitive password is a series of challenge questions about facts or predefined responses that only the subject should know. Authentication systems often collect the answers to these questions during the initial registration of the account, but they can be collected or modified later. As an example, the subject might be asked three to five questions such as these when creating an account:

- What is your birth date?
- What is your mother's maiden name?
- What is the name of your first boss?
- What is the name of your first pet?
- What is your favorite sport?

Smartcards and Tokens

Smartcards

A *smartcard* is a credit card–sized ID or badge and has an integrated circuit chip embedded in it. Smartcards contain information about the authorized user that is used for identification and/or authentication purposes.

Tokens

A *token device*, or hardware token, is a password-generating device that users can carry with them. A common token used today includes a display that shows a six- to eight-digit number. An authentication server stores the details of the token, so at any moment, the server knows what number is displayed on the user's token.

Access Criteria

Granting access rights to subjects should be based on the level of trust a company has in a subject and the subject's need to know. Using ***roles*** is an efficient way to assign rights to a type of user who performs a certain task.

Using ***groups*** is another effective way of assigning access control rights. If several users require the same type of access to information and resources, putting them into a group and then assigning rights and permissions to that group is easier to manage than assigning rights and permissions to each and every individual separately.

Physical or logical location can also be used to restrict access to resources. Some files may be available only to users who can log on interactively to a computer. This means the user must be physically at the computer and enter the credentials locally versus logging on remotely from another computer.

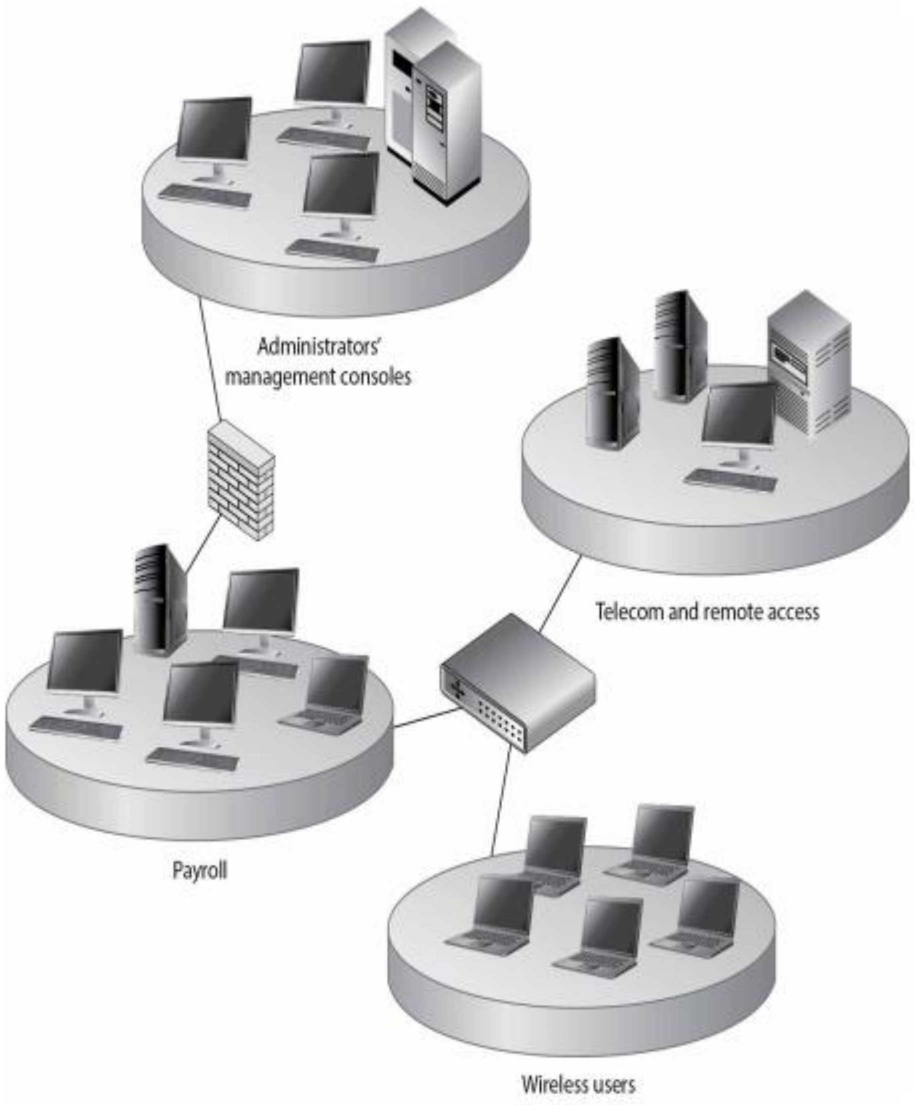
Logical location restrictions are usually done through network address restrictions.

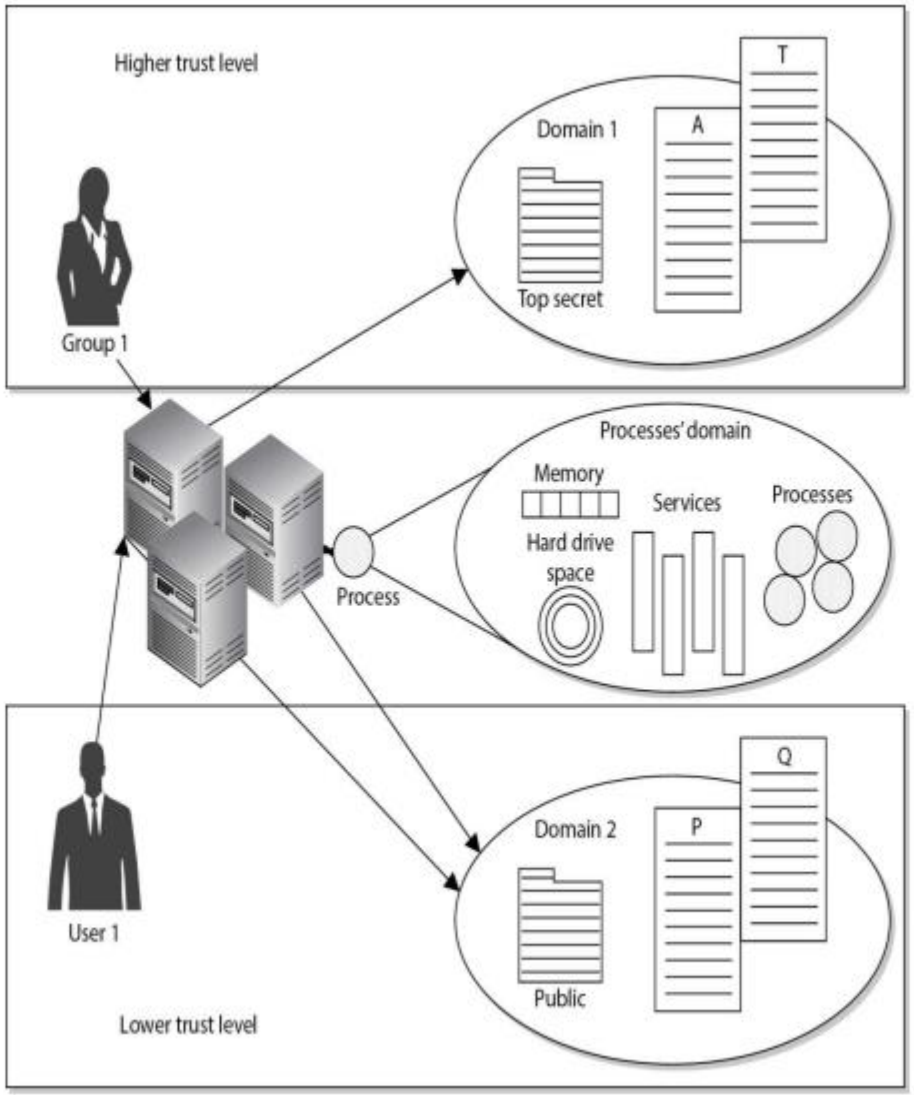
Time of day, or temporal isolation, is another access control mechanism that can be used. If a security professional wants to ensure no one is accessing payroll files between the hours of 8:00 p.m. and 4:00 a.m., she can implement that configuration to ensure access at these times is restricted.

Transaction-type restrictions can be used to control what data is accessed during certain types of functions and what commands can be carried out on the data. An online banking program may allow a customer to view his account balance, but may not allow the customer to transfer money until he has a certain security level or access right.

Default to No Access

Access control mechanisms should default to no access so as to provide the necessary level of security and ensure no security holes go unnoticed.


Administrators' management consoles
Telecom and remote access
Payroll
Wireless users


Higher trust level
T
Domain 1
A
Top secret
Group 1
Processes' domain
Memory
Services
Processes
Hard drive space
Process
Q
Domain 2
P
User 1
Public
Lower trust level

Facilities Case: Department of Homeland Security

1. What distinct roles can you locate within the physical access control systems (PACS) application’s four areas? What are general security roles that can be used as placeholders for the PACS application roles?
2. Name the logical or physical systems that are described in the PACS application.
3. What assumptions could you make about the nature of the information related to identification in the PACS application cited below?

Module 2

Identity and Access Provisioning Lifecycle

Module Objectives

1. Define the process of user and systems access review.
2. Apply the appropriate control types/categories for provisioning and deprovisioning of identities.

User Access Review

- Enforces security policy
- Continues over the lifecycle of access
- Mitigates vulnerabilities associated with aggregation
- Concludes with termination of access

System Account Access Review

- Presents often-exploited vulnerability for attackers
- Securing begins with renaming account
- Some system accounts further complicated by being service accounts

Provisioning and Deprovisioning

- Provision a user account and apply user permissions
- Modify user permissions
- Deprovision user account and end user permissions

Activity: Identify the Roles and Control Types and Categories of Provisioning and Deprovisioning

INSTRUCTIONS

Working together in small teams, answer the questions below.

- What additional controls (choose from the CIA triad) could be added to each of the three phases of the process flow?
  - Add control types
  - Add control categories
- What roles can you identify in the process flow (i.e., Custodian, Data Owner, etc.)?

Module 3

Identification and Authentication of People, Devices, and Services

Module Objectives

1. Classify various identification, authentication, and authorization technologies for use in managing people, devices, and services.

Identity Management Implementation

These are the four elements of identity management implementation:

Identification

Authentication

Authorization

Accountability

MANAGE IDENTIFICATION AND AUTHENTICATION OF PEOPLE, DEVICES, AND SERVICES

Identification is the process of verifying that a claimed identity is valid. For example, identification occurs when a person supplies a user ID and a system verifies that the user ID is valid. (This step does not prove that the person is who they claim to be, but only that such an identity has been established.)

Authentication is the validation of a provable assertion of an identity. For example, when a person uses a user ID, they are required to provide their password as a way to prove that they actually are the owner of that user ID.

Although authentication proves that a person is who they claim to be, that is not the same as proving they have the right to do whatever they are trying to do. For example, a person might be a validly authenticated member of an organization, but that doesn't necessarily mean they have access to all of that organization's accounting or human resources files. *Authorization* is the process of determining whether to allow a person to have access to resources.

MANAGE IDENTIFICATION AND AUTHENTICATION OF PEOPLE, DEVICES, AND SERVICES

The final stage of the identity lifecycle is sometimes referred to as *deprovisioning*, *disabling*, *revocation*, and other terms, but it generally means ending a person’s general access to the system. However, that person’s formal identity will often persist within the system for months or years after the person it was created for has no direct need for it. For example, a bank will have archives of a member who closed an account, and an organization will keep records of former employees for taxes, human resources, and regulatory purposes.

MANAGE IDENTIFICATION AND AUTHENTICATION OF PEOPLE, DEVICES, AND SERVICES

SINGLE FACTOR/MULTIFACTOR AUTHENTICATION

Authentication—the process of proving that a person or system is who they claim to be—has traditionally been based on one or more of three authentication factors:

Type I: Something you know (e.g., a password)
Type II: Something you have (e.g., a smartcard)
Type III: Something you are (e.g., your fingerprint)
Two emerging technologies have recently been coming into greater prominence as authentication factors as well: “something you do” and “somewhere you are.”

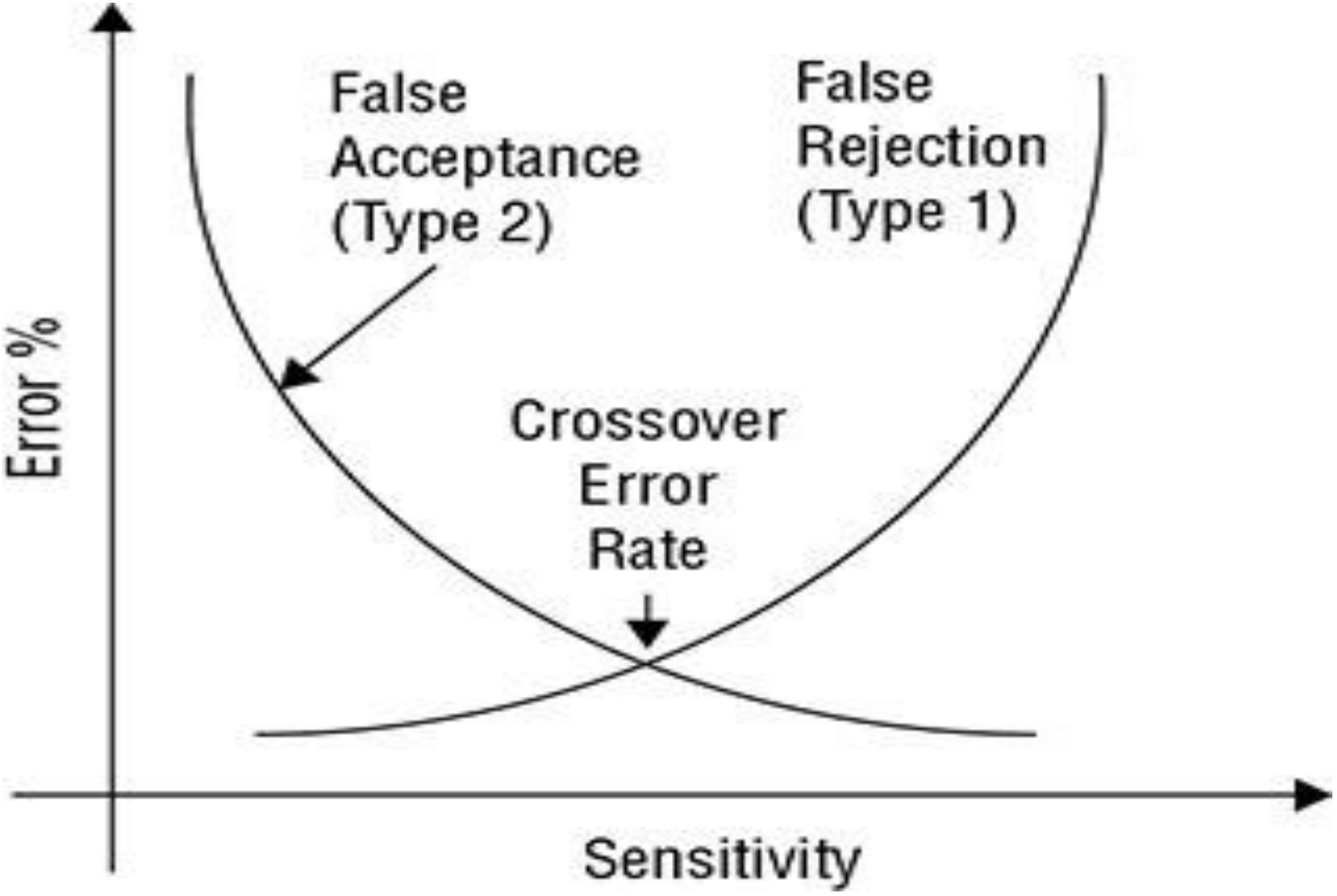
Single-factor authentication involves the use of exactly one of these three factors to carry out the authentication process being requested. ***Multifactor authentication*** helps to ensure that a user is who he or she claims to be via the use of more than one factor to carry out the authentication process being requested.

MANAGE IDENTIFICATION AND AUTHENTICATION OF PEOPLE, DEVICES, AND SERVICES

Synchronous dynamic password tokens are time-based, changing to a different number sequence after a specified period of time (say, once a minute). The software on the authenticating system also “knows” the sequence and the timing of changes, and so offers a window to the user during which the number displayed on the token will validate access.

Asynchronous dynamic password tokens do not rely on synchronized time. Rather, each side of the login sequence keeps track of a counter, generating the next one-time password by using the same algorithm to produce the same sequence for that count.

MANAGE IDENTIFICATION AND AUTHENTICATION OF PEOPLE, DEVICES, AND SERVICES



Accountability is the attribute of a security architecture that allows individuals and processes to be held responsible for their actions and decisions. It ensures that account management has assurance that only authorized users are accessing the system and using it properly.

SESSION MANAGEMENT

A *session* is a series of exchanges between two entities, perhaps a human user and a web server. Session management entails initiating, controlling, maintaining, and terminating the “state” of these exchanges.

The web surfing protocols Hypertext Transfer Protocol (HTTP) and HyperText Transfer Protocol Secure (HTTPS) are conducted statelessly. This means that each request to a web server for information is handled with no knowledge of previous requests. This “stateless” operation was part of the original design of the World Wide Web. However, as the Web exploded in popularity and commercial applications were created for it, the need for some information (like the contents of a virtual shopping cart) to persist through a series of back-and-forth exchanges with a website became apparent

Session *sidejacking* can be accomplished by using a packet sniffer (or other eavesdropping technique) to intercept and study the traffic between the two sides. Many sites revert to plain-text exchanges, even in Secure Socket Layer (SSL) sessions, after authentication is complete. The password probably will not be passed in plain text, but the session token (or *cookie*) may be, and this may be enough for impersonation to begin.

Identity Assurance Levels

NIST Special Publication 800-63A, “Digital Identity Guidelines: Enrollment and Identity Proofing Requirements” suggests you consider three “identity assurance levels” (IALs).

At risk level 1, you as a credential service provider can take “self-asserted” attributes (assertions from the claimant) at face value, neither validated nor verified.

At risk level 2, you will require evidence that “supports the real-world existence” of the claimed identity and then use that evidence to verify that the claimant has a right to that identity. The evidence could be a state-supplied driver’s license, for instance, or a certified copy of a birth certificate.

At risk level 3, you should require the physical presence of the claimant. They must present themselves to you, and any identifying attributes must be verified by you. This applies to physical measurements, biometric attributes, and other characteristics (such as birth date) that can be established by your validation of original documents.

MANAGE IDENTIFICATION AND AUTHENTICATION OF PEOPLE, DEVICES, AND SERVICES

IMPACT CATEGORIES	IAL1	IAL2	IAL3
Inconvenience, distress, or damage to standing or reputation	Low	Med	High
Financial loss or company liability	Low	Med	High
Harm to company programs or shareholder interests	N/A	Low/Med	High
Unauthorized release of sensitive information	N/A	Low/Med	High
Personal safety	N/A	Low	Med/High
Civil or criminal violations	N/A	Low/Med	High

TABLE 5.1 **Sample Identity Assurance Levels**

MANAGE IDENTIFICATION AND AUTHENTICATION OF PEOPLE, DEVICES, AND SERVICES

REQUIREMENT	IAL1	IAL2	IAL3
Presence	No requirements	In-person and unsupervised remote.	In-person and supervised remote
Resolution	No requirements	The minimum attributes necessary to accomplish identity resolution Knowledge-based verification may be used for added confidence.	Same as IAL2
Evidence	No identity evidence is collected.	One piece of SUPERIOR or STRONG evidence depending on strength of original proof and validation occurs with issuing source, or Two pieces of STRONG evidence, or One piece of STRONG evidence plus two pieces of FAIR evidence	Two pieces of SUPERIOR evidence, or One piece of SUPERIOR evidence and one piece of STRONG evidence depending on strength of original proof and validation occurs with issuing source, or Two pieces of STRONG evidence plus one piece of FAIR evidence
Validation	No validation	Each piece of evidence must be validated with a process that is able to achieve the same strength as the evidence presented.	Same as IAL2
Verification	No verification	Verified by a process that is able to achieve a strength of STRONG	Verified by a process that is able to achieve a strength of SUPERIOR
Address confirmation	No requirements for address confirmation	Required. Enrollment code sent to any address of record. Notification sent by means different from enrollment code	Required. Notification of proofing to postal address
Biometric collection	No.	Optional	Mandatory

MANAGE IDENTIFICATION AND AUTHENTICATION OF PEOPLE, DEVICES, AND SERVICES

Digital Certificates

A *digital certificate* is an electronic credential, a document that makes use of modern public key cryptography to provide a means of verifying an identity. It may help to think of a certificate as a driver's license made up of encrypted ones and zeros, bound to an electronically stored identity.

Various circumstances might invalidate a certificate, such as the following:

- Change of the subject's name (does not always invalidate the certificate, depending on policy and the implementing technology)
- Change of association between the subject and the certificate authority (such as when the subject is an employee leaving the company that acts as the certificate authority)
- Compromise of the private key that corresponds to the public key included in the certificate

MANAGE IDENTIFICATION AND AUTHENTICATION OF PEOPLE, DEVICES, AND SERVICES

Biometrics

- **Fingerprints**
- **Face Scans**
- **Retina Scans**
- **Iris Scans**
- **Palm Scans**
- **Hand Geometry**
- **Heart/Pulse Patterns**
- **Voice Pattern Recognition**
- **Signature Dynamics**
- **Keystroke Patterns**

Biometric Factor Error Ratings

- *False Rejection Rate or Type I error.*
- *False Acceptance Rate or Type II error*.

Biometric Registration

- *Multifactor Authentication*
- *Device Authentication*
- *Service Authentication*

Implementing Identity Management

Identity management techniques generally fall into one of two categories: centralized and decentralized/distributed.

- *Centralized access control* implies that all authorization verification is performed by a single entity within a system.
- *Decentralized access control* (also known as *distributed access control*) implies that various entities located throughout a system perform authorization verification.

Single Sign-On

Single sign-on (SSO) is a centralized access control technique that allows a subject to be authenticated once on a system and to access multiple resources without authenticating again. For example, users can authenticate once on a network and then access resources throughout the network without being prompted to authenticate again.

LDAP and Centralized Access Control

Within a single organization, a centralized access control system is often used. For example, a *directory service* is a centralized database that includes information about subjects and objects. Many directory services are based on the Lightweight Directory Access Protocol (LDAP). For example, the Microsoft Active Directory Domain Services is LDAP-based.

LDAP and PKIs

A public-key infrastructure (PKI) uses LDAP when integrating digital certificates into transmissions. Chapter 7 covers a PKI in more depth, but in short, a PKI is a group of technologies used to manage digital certificates during the certificate lifecycle. There are many times when clients need to query a certificate authority (CA) for information on a certificate, and LDAP is one of the protocols used.

LDAP and centralized access control systems can be used to support single sign-on capabilities.

Kerberos

Key Distribution Center The *key distribution center (KDC)* is the trusted third party that provides authentication services. Kerberos uses symmetric-key cryptography to authenticate clients to servers. All clients and servers are registered with the KDC, and it maintains the secret keys for all network members.

Kerberos Authentication Server The authentication server hosts the functions of the KDC: a ticket-granting service (TGS) and an authentication service (AS). However, it is possible to host the ticket-granting service on another server. The *authentication service* verifies or rejects the authenticity and timeliness of tickets. This server is often called the KDC.

Ticket-Granting Ticket A ticket-granting ticket (TGT) provides proof that a subject has authenticated through a KDC and is authorized to request tickets to access other objects. A TGT is encrypted and includes a symmetric key, an expiration time, and the user’s IP address. Subjects present the TGT when requesting tickets to access objects.

Ticket A ticket is an encrypted message that provides proof that a subject is authorized to access an object. It is sometimes called a service ticket (ST). Subjects request tickets to access objects, and if they have authenticated and are authorized to access the object, Kerberos issues them a ticket. Kerberos tickets have specific lifetimes and usage parameters. Once a ticket expires, a client must request a renewal or a new ticket to continue communications with any server.

The Kerberos logon process works as follows:

1. The user types a username and password into the client.
2. The client encrypts the username with AES for transmission to the KDC.
3. The KDC verifies the username against a database of known credentials.
4. The KDC generates a symmetric key that will be used by the client and the Kerberos server. It encrypts this with a hash of the user’s password. The KDC also generates an encrypted time-stamped TGT.
5. The KDC then transmits the encrypted symmetric key and the encrypted time-stamped TGT to the client.
6. The client installs the TGT for use until it expires. The client also decrypts the symmetric key using a hash of the user’s password.

The following steps are involved in this process:

1. The client sends its TGT back to the KDC with a request for access to the resource.
2. The KDC verifies that the TGT is valid and checks its access control matrix to verify that the user has sufficient privileges to access the requested resource.
3. The KDC generates a service ticket and sends it to the client.
4. The client sends the ticket to the server or service hosting the resource.
5. The server or service hosting the resource verifies the validity of the ticket with the KDC.
6. Once identity and authorization is verified, Kerberos activity is complete. The server or service host then opens a session with the client and begins communications or data transmission.

Federated Identity Management and SSO

SSO is common on internal networks, and it also used on the internet. Many cloud-based applications use an SSO solution, making it easier for users to access resources over the internet. Many cloud-based applications use federated identity management (FIM), which is a form of SSO.

Hypertext Markup Language Hypertext Markup Language (HTML) is commonly used to display static web pages. HTML was derived from the Standard Generalized Markup Language (SGML) and the Generalized Markup Language (GML). HTML describes how data is displayed using tags to manipulate the size and color of the text. For example, the following H1 tag displays the text as a level one heading: <H1>I Passed The CISSP Exam</H1>.

Extensible Markup Language *Extensible Markup Language (XML)* goes beyond describing how to display the data by actually describing the data. XML can include tags to describe data as anything desired. For example, the following tag identifies the data as the results of taking an exam: <ExamResults>Passed</ExamResults>.

Security Assertion Markup Language *Security Assertion Markup Language (SAML)* is an XML-based language that is commonly used to exchange authentication and authorization (AA) information between federated organizations. It is often used to provide SSO capabilities for browser access.

Service Provisioning Markup Language *Service Provisioning Markup Language (SPML)* is a newer framework developed by OASIS, a nonprofit consortium that encourages development of open standards. It is based on XML and is specifically designed for exchanging user information for federated identity SSO purposes. It is based on the Directory Service Markup Language (DSML), which can display LDAP-based directory service information in an XML format.

Extensible Access Control Markup Language *Extensible Access Control Markup Language (XACML)* is a standard developed by OASIS and is used to define access control policies within an XML format. It commonly implements policies as an attribute-based access control system but can also use role-based access controls. It helps provide assurances to all members in a federation that they are granting the same level of access to different roles.

OAuth 2.0 OAuth (implying open authentication) is an open standard used for access delegation. As an example, imagine you have a Twitter account. You then download an app called Acme that can interact with your Twitter account. When you try to use this feature, it redirects you to Twitter, and if you’re not already logged on, you’re prompted to log on to Twitter. Twitter then asks you if you want to authorize the app and tells you what permissions you are granting. If you approve, the Acme app can access your Twitter account. A primary benefit is that you never provide your Twitter credentials to the Acme app. Even if the Acme app suffers a major data breach exposing all their data, it does not expose your credentials. Many online sites support OAuth 2.0, but not OAuth 1.0. OAuth 2.0 is not backward compatible with OAuth 1.0. RFC 6749 documents OAuth 2.0.

OpenID OpenID is also an open standard, but it is maintained by the OpenID Foundation rather than as an RFC standard. It provides decentralized authentication, allowing users to log into multiple unrelated websites with one set of credentials maintained by a third-party service referred to as an OpenID provider.

OpenID Connect OpenID Connect is an authentication layer using the OAuth 2.0 framework. Like OpenID, it is maintained by the OpenID Foundation.

Scripted Access

Scripted access or logon scripts establish communication links by providing an automated process to transmit logon credentials at the start of a logon session.

Credential Management Systems

A *credential management system* provides a storage space for users to keep their credentials when SSO isn’t available.

Integrating Identity Services

OpenID OpenID is also an open standard, but it is maintained by the OpenID Foundation rather than as an RFC standard. It provides decentralized authentication, allowing users to log into multiple unrelated websites with one set of credentials maintained by a third-party service referred to as an OpenID provider.

OpenID Connect OpenID Connect is an authentication layer using the OAuth 2.0 framework. Like OpenID, it is maintained by the OpenID Foundation.

Scripted Access

Scripted access or logon scripts establish communication links by providing an automated process to transmit logon credentials at the start of a logon session.

Credential Management Systems

A *credential management system* provides a storage space for users to keep their credentials when SSO isn't available.

Integrating Identity Services

OpenID OpenID is also an open standard, but it is maintained by the OpenID Foundation rather than as an RFC standard. It provides decentralized authentication, allowing users to log into multiple unrelated websites with one set of credentials maintained by a third-party service referred to as an OpenID provider.

OpenID Connect OpenID Connect is an authentication layer using the OAuth 2.0 framework. Like OpenID, it is maintained by the OpenID Foundation.

Scripted Access

Scripted access or logon scripts establish communication links by providing an automated process to transmit logon credentials at the start of a logon session.

Credential Management Systems

A *credential management system* provides a storage space for users to keep their credentials when SSO isn’t available.

Integrating Identity Services

AAA Protocols

Several protocols provide authentication, authorization, and accounting and are referred to as AAA protocols. These provide centralized access control with remote access systems such as virtual private networks (VPNs) and other types of network access servers.

RADIUS

Remote Authentication Dial-in User Service (RADIUS) centralizes authentication for remote connections. It is typically used when an organization has more than one network access server (or remote access server). A user can connect to any network access server, which then passes on the user's credentials to the RADIUS server to verify authentication and authorization and to track accounting. In this context, the network access server is the RADIUS client and a RADIUS server acts as an authentication server. The RADIUS server also provides AAA services for multiple remote access servers.

TACACS+

Terminal Access Controller Access-Control System (TACACS) was introduced as an alternative to RADIUS. Cisco later introduced extended TACACS (XTACACS) as a proprietary protocol. However, TACACS and XTACACS are not commonly used today. TACACS Plus (TACACS+) was later created as an open publicly documented protocol, and it is the most commonly used of the three.

TACACS+ provides several improvements over the earlier versions and over RADIUS. It separates authentication, authorization, and accounting into separate processes, which can be hosted on three separate servers if desired. The other versions combine two or three of these processes. Additionally, TACACS+ encrypts all of the authentication information, not just the password as RADIUS does. TACACS and XTACACS use UDP port 49, while TACACS+ uses Transmission Control Protocol (TCP) port 49, providing a higher level of reliability for the packet transmissions.

Diameter

Building on the success of RADIUS and TACACS+, an enhanced version of RADIUS named Diameter was developed. It supports a wide range of protocols, including traditional IP, Mobile IP, and Voice over IP (VoIP). Because it supports extra commands, it is becoming popular in situations where roaming support is desirable, such as with wireless devices and smartphones. While Diameter is an upgrade to RADIUS, it is not backward compatible to RADIUS.

Diameter uses TCP port 3868 or Stream Control Transmission Protocol (SCTP) port 3868, providing better reliability than UDP used by RADIUS. It also supports Internet Protocol ***security (IPsec) and Transport Layer Security (TLS) for encryption.***

Managing the Identity and Access Provisioning Lifecycle

- **Provisioning**
- **Account Review**
- **Account Revocation**

RADIUS vs. TACACS+

	RADIUS	TACACS+
Protocol and Port(s) Used	UDP: 1812 & 1813 -or- UDP: 1645 & 1646	TCP: 49
Encryption	Encrypts only the Password Field	Encrypts the entire payload
Authentication & Authorization	Combines Authentication and Authorization	Separates Authentication & Authorization
Primary Use	Network Access	Device Administration

Diameter

Diameter is a protocol that has been developed to build upon the functionality of RADIUS and overcome many of its limitations. The creators of this protocol decided to call it Diameter as a play on the term RADIUS—as in *the diameter is twice the radius.*

Diameter protocol consists of two portions. The first is the base protocol, which provides the secure communication among Diameter entities, feature discovery, and version negotiation. The second is the extensions, which are built on top of the base protocol to allow various technologies to use Diameter for authentication.

Diameter is a peer-based protocol that allows either end to initiate communication. This functionality allows the Diameter server to send a message to the
access server to request the user to provide another authentication credential if she is attempting to access a secure resource.

Diameter provides the AAA functionality, as listed next.

Authentication:

- PAP, CHAP, EAP
- End-to-end protection of authentication information
- Replay attack protection

Authorization:

- Redirects, secure proxies, relays, and brokers
- State reconciliation
- Unsolicited disconnect
- Reauthorization on demand

Accounting:

- Reporting, roaming operations (ROAMOPS) accounting, event monitoring

Comparing Permissions, Rights, and Privileges

Permissions In general, permissions refer to the access granted for an object and determine what you can do with it.

Rights A right primarily refers to the ability to take an action on an object.

Privileges *Privileges* are the combination of rights and permissions. For example, an administrator for a computer will have full privileges, granting the administrator full rights and permissions on the computer. The administrator will be able to perform any actions and access any data on the computer.

Understanding Authorization Mechanisms

Implicit Deny A basic principle of access control is *implicit deny* and most authorization mechanisms use it.

Access Control Matrix An *access control matrix* is a table that includes subjects, objects, and assigned privileges.

Capability Tables *Capability tables* are another way to identify privileges assigned to subjects. They are different from ACLs in that a capability table is focused on subjects.

Access control lists (ACLs) are used in several operating systems, applications, and router configurations.

Constrained Interface Applications use *constrained interfaces* or restricted interfaces to restrict what users can do or see based on their privileges. Users with full privileges have access to all the capabilities of the application.

Content-Dependent Control *Content-dependent access controls* restrict access to data based on the content within an object.

Context-Dependent Control *Context-dependent access controls* require specific activity before granting users access.

Comparing Permissions, Rights, and Privileges

Permissions In general, permissions refer to the access granted for an object and determine what you can do with it.

Rights A right primarily refers to the ability to take an action on an object.

Privileges *Privileges* are the combination of rights and permissions. For example, an administrator for a computer will have full privileges, granting the administrator full rights and permissions on the computer. The administrator will be able to perform any actions and access any data on the computer.

Understanding Authorization Mechanisms

Implicit Deny A basic principle of access control is *implicit deny* and most authorization mechanisms use it.

Access Control Matrix An *access control matrix* is a table that includes subjects, objects, and assigned privileges.

Capability Tables *Capability tables* are another way to identify privileges assigned to subjects. They are different from ACLs in that a capability table is focused on subjects.

Constrained Interface Applications use *constrained interfaces* or restricted interfaces to restrict what users can do or see based on their privileges. Users with full privileges have access to all the capabilities of the application.

Content-Dependent Control *Content-dependent access controls* restrict access to data based on the content within an object.

Context-Dependent Control *Context-dependent access controls* require specific activity before granting users access.

Need to Know This principle ensures that subjects are granted access only to what they *need to know* for their work tasks and job functions. Subjects may have clearance to access classified or restricted data but are not granted authorization to the data unless they actually need it to perform a job.

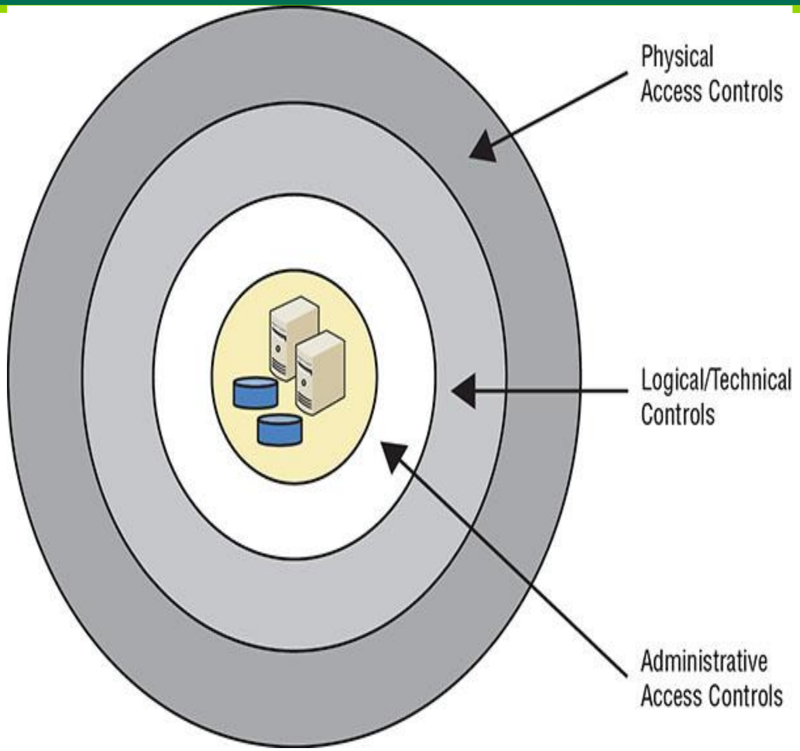
Least Privilege The *principle of least privilege* ensures that subjects are granted only the privileges they need to perform their work tasks and job functions. This is sometimes lumped together with need to know. The only difference is that least privilege will also include rights to take action on a system.

Separation of Duties and Responsibilities The *separation of duties and responsibilities* principle ensures that sensitive functions are split into tasks performed by two or more employees. It helps to prevent fraud and errors by creating a system of checks and balances.

Defining Requirements with a Security Policy

A security policy is a document that defines the security requirements for an organization. It identifies assets that need protection and the extent to which security solutions should go to protect them.

Implementing Defense in Depth



The concept of defense in depth highlights several important points:

- An organization’s security policy, which is one of the administrative access controls, provides a layer of defense for assets by defining security requirements.
- Personnel are a key component of defense. However, they need proper training and education to implement, comply with, and support security elements defined in an organization’s security policy.
- A combination of administrative, technical, and physical access controls provides a much stronger defense. Using only administrative, only technical, or only physical controls results in weaknesses that attackers can discover and exploit.

Session Management

RFC 2965 provides an example of session management with cookies. All transaction requests are maintained and tracked as a user engages requests from a website.

Registration and Proofing of Identity

NIST SP 800-63-3 contains three levels of assurance for digital identities:

IAL1: Self-asserted

IAL2: Remote or in-person

IAL3: Verified by authorized credential service provider

Module 4

Identity Management Implementation

Module Objectives

1. Differentiate the languages and protocols that are related to roles and systems that support federation.
2. Select the appropriate components for a federated environment relevant to business requirements.

Federated Identity Management (FIM)

- **Federated Identity Management (FIM)** is specified and sought for use between different organizations or entities that need to share resources or have users in common.
- Services that provide federation:
  - Security Assertion Markup Language (SAML)
  - Open Authorization (OAuth)

Federated Identity Management (FIM)

Using SAML for Federated Identity Management

SAML, a modern open standard defined by the OASIS Committee, was discussed earlier in the “Identity Management Implementation” section. Under federated identity management, XML-based SAML makes use of three *roles* and four primary *components*.

In its simplest application within IAM, SAML provides a formal mechanism and format for one entity to assure a second entity about the identity of a third, usually a human being. These three SAML roles include the following:

- **Identity provider (IdP):** This is the first entity. It makes an assertion about another identity, based on information it has. This information might have just been obtained, say by querying the user for a username/password pair.
- **Service provider (SP):** This entity is the relying party that is being asked to provide its service or resource, based on the assurance provided by the IdP.
- **Subject or principal:** This entity is the subject of the assertion, usually a person, who is in some sense being vouched for.

Federated Identity Management (FIM)

The four primary components of SAML are:

- **Assertions:** In a SAML assertion, an identity provider makes one or more statements about a subject (also known as the *principal*—usually, a user) that the relying party can use to make access control decisions. The statement vouches for the authentication of the subject (perhaps providing details in an *authentication statement*) and may provide one or more *attribute statements*, describing the subject by means of name-value pairs. The assertion may also specify, in an *authorization decision statement*, conditions under which the principal is permitted to perform certain actions on a given resource.
- **Protocols:** SAML protocols describe how information is to be exchanged between, or consumed by, SAML entities. These rules specify the format and content of several types SAML exchanges, especially queries between entities. For example, SAML version 1.1 provides for queries concerning the kind of authentication, attribute, and authorization information contained in assertions. Additional protocols, added in SAML 2.0, include an Artifact Resolution Protocol, a Name Identifier Management Protocol, and Single Logout Protocol.
- **Bindings:** SAML *bindings* specify how to encapsulate the various SAML protocols in various types of messages. Since SAML 2.0, these bindings have described not only how to include queries in, for example, SOAP envelopes, but also HTTP POST and GET exchanges (among others).
- **Profiles:** SAML bindings, protocols, and assertions can be pulled together to make a *profile*, a set of definitions and instructions for a specified use case. SAML 2.0, for instance, makes available five different profiles for SSO use cases: Enhanced Client or Proxy (ECP), Identity Provider Discovery, Name Identifier Management, Single Logout, and Web Browser SSO. Several other profiles are available in SAML 2.0. There are third-party profiles, too, such as the OASIS WS-Security SAML Token Profile.

Federated Identity Management (FIM)

Authentication and Authorization Methods

RADIUS

TACAS

TACACS+

DIAMeter

Federated Identity Management (FIM)

The four primary components of SAML are:

- **Assertions:** In a SAML assertion, an identity provider makes one or more statements about a subject (also known as the *principal*—usually, a user) that the relying party can use to make access control decisions. The statement vouches for the authentication of the subject (perhaps providing details in an *authentication statement*) and may provide one or more *attribute statements*, describing the subject by means of name-value pairs. The assertion may also specify, in an *authorization decision statement*, conditions under which the principal is permitted to perform certain actions on a given resource.
- **Protocols:** SAML protocols describe how information is to be exchanged between, or consumed by, SAML entities. These rules specify the format and content of several types SAML exchanges, especially queries between entities. For example, SAML version 1.1 provides for queries concerning the kind of authentication, attribute, and authorization information contained in assertions. Additional protocols, added in SAML 2.0, include an Artifact Resolution Protocol, a Name Identifier Management Protocol, and Single Logout Protocol.
- **Bindings:** SAML *bindings* specify how to encapsulate the various SAML protocols in various types of messages. Since SAML 2.0, these bindings have described not only how to include queries in, for example, SOAP envelopes, but also HTTP POST and GET exchanges (among others).
- **Profiles:** SAML bindings, protocols, and assertions can be pulled together to make a *profile*, a set of definitions and instructions for a specified use case. SAML 2.0, for instance, makes available five different profiles for SSO use cases: Enhanced Client or Proxy (ECP), Identity Provider Discovery, Name Identifier Management, Single Logout, and Web Browser SSO. Several other profiles are available in SAML 2.0. There are third-party profiles, too, such as the OASIS WS-Security SAML Token Profile.

Federated Identity Management (FIM)

Federated Identity Management (FIM)

Federated Identity Management (FIM)

Federated Identity Management (FIM)

Security Assertion Markup Language (SAML) Roles

Roles:

- Identity provider (IdP)
- Service provider/relying party
- User/principal

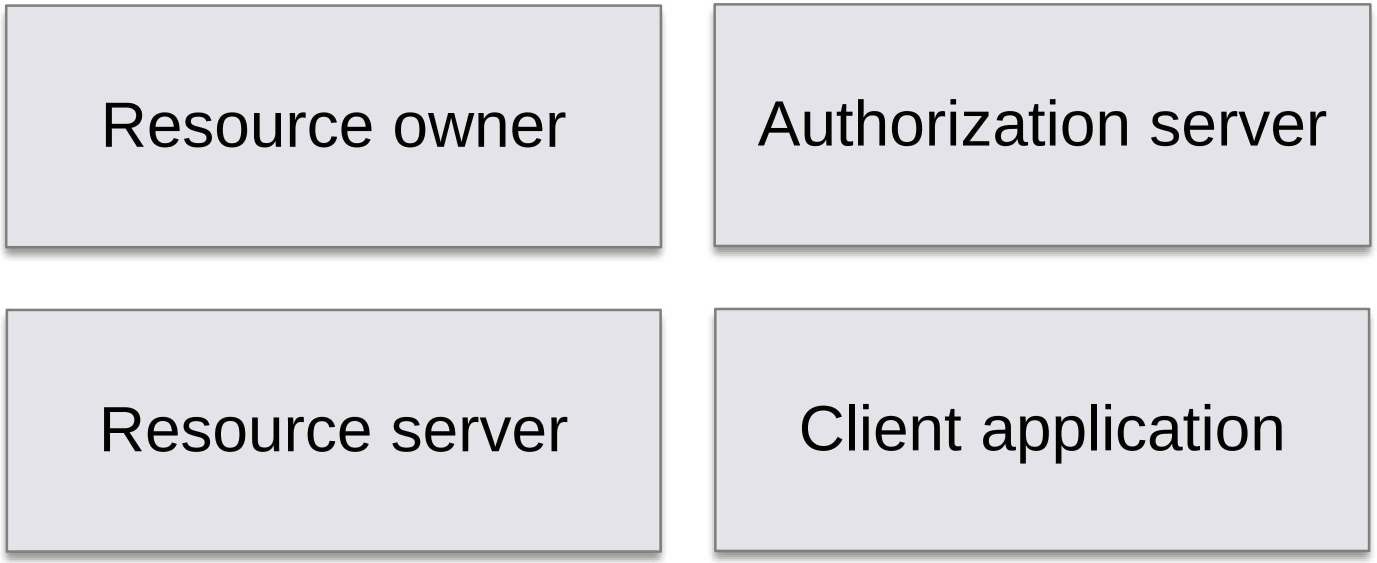
Security Assertion Markup Language (SAML) Components

Components:

- Assumptions
- Bindings
- Protocols
- Profiles

Open Authentication

Roles:



Resource owner

Authorization server

Resource server

Client application

Integrate Identity Management as a Third-Party Service

- On-Premise
- Cloud

Activity: Select the Appropriate Components for a Federated Environment Linking Two or More Companies’ Discrete Resources

INSTRUCTIONS

As a team, reflect upon and discuss actual business needs within your corporation.

- Each team should allow every participant to relate business needs within each company.
- Instead of contributing to or jumping to a conclusion on what solution there might be, each participant should ask deeper questions of the presenter to uncover additional insights into the environment.
- Expose assumptions by asking “why” a thing is so or to give an example of a statement shared.
- Create a business case for utilizing either OAuth or SAML or both. What are actual business drivers?
- Also select if it should be solved on-premise or in the cloud and why.
- Create analogous connections between the roles in SAML and OAuth.

Module 5

Implement and Manage Authorization Mechanisms

Module Objectives

1. Appraise various access control models to meet business security requirements.

Types of Access Control

NIST SP 800-192 specifies the following types of access control:

- Discretionary access control (DAC)
- Mandatory access control (MAC)
- Nondiscretionary access control (NDAC)
- Role-based access control (RBAC)
- Rule-based access control (RBAC)
- Attribute-based access control (ABAC)

Understanding Access Control Attacks

Identifying Assets

Asset valuation refers to identifying the actual value of assets with the goal of prioritizing them. Risk management focuses on assets with the highest value and identifies controls to mitigate risks to these assets.

Identifying Threats

After identifying and prioritizing assets, an organization attempts to identify any possible threats to the valuable systems. *Threat modeling* refers to the process of identifying, understanding, and categorizing potential threats. A goal is to identify a potential list of threats to these systems and to analyze the threats.

Identifying Vulnerabilities

After identifying valuable assets and potential threats, an organization will perform *vulnerability analysis*. In other words, it attempts to discover weaknesses in these systems against potential threats. In the context of access control, vulnerability analysis attempts to identify the strengths and weaknesses of the different access control mechanisms and the potential of a threat to exploit a weakness.

Types of Access Control

MAC model use one of the following three types of environments:

Hierarchical Environment *A hierarchical environment* relates various classification labels in an ordered structure from low security to medium security to high security, such as Confidential, Secret, and Top Secret, respectively. Each level or classification label in the structure is related. Clearance in one level grants the subject access to objects in that level as well as to all objects in lower levels but prohibits access to all objects in higher levels. For example, someone with a Top Secret clearance can access Top Secret data and Secret data.

Compartmentalized Environment In a *compartmentalized environment*, there is no relationship between one security domain and another. Each domain represents a separate isolated compartment. To gain access to an object, the subject must have specific clearance for its security domain.

Hybrid Environment A *hybrid environment* combines both hierarchical and compartmentalized concepts so that each hierarchical level may contain numerous subdivisions that are isolated from the rest of the security domain. A subject must have the correct clearance and the need to know data within a specific compartment to gain access to the compartmentalized object. A hybrid MAC environment provides granular control over access, but becomes increasingly difficult to manage as it grows.

Types of Access Control

Threat Modeling Approaches

Focused on Assets This method uses asset valuation results and attempts to identify threats to the valuable assets. Personnel evaluate specific assets to determine their susceptibility to attacks. If the asset hosts data, personnel evaluate the access controls to identify threats that can bypass authentication or authorization mechanisms.

Focused on Attackers Some organizations identify potential attackers and identify the threats they represent based on the attacker's goals. For example, a government is often able to identify potential attackers and recognize what the attackers want to achieve. They can then use this knowledge to identify and protect their relevant assets. This is becoming increasingly more difficult, though, with so many APTs sponsored by foreign nation states.

Focused on Software If an organization develops software, it can consider potential threats against the software. While organizations didn't commonly develop their own software years ago, it's common to do so today. Specifically, most organizations have a web presence, and many create their own websites. Fancy websites attract more traffic, but they also require more sophisticated programming and present additional threats.

Types of Access Control

Common Access Control Attacks

Access Aggregation Attacks

Access aggregation refers to collecting multiple pieces of nonsensitive information and combining (i.e., aggregating) them to learn sensitive information. In other words, a person or group may be able to collect multiple facts about a system and then use these facts to launch an attack.

Combining defense-in-depth, need-to-know, and least privilege principles helps prevent access aggregation attacks.

Password Attacks

Passwords are the weakest form of authentication, and there are many password attacks available. If an attacker is successful in a password attack, the attacker can gain access to the account and access resources authorized to the account.

Dictionary Attacks

A *dictionary attack* is an attempt to discover passwords by using every possible password in a predefined database or list of common or expected passwords.

Brute-Force Attacks

A *brute-force attack* is an attempt to discover passwords for user accounts by systematically attempting all possible combinations of letters, numbers, and symbols. Attackers don’t typically type these in manually but instead have programs that can programmatically try all the combinations. A *hybrid attack* attempts a dictionary attack and then performs a type of brute-force attack with one-upped-constructed passwords.

Types of Access Control

The following three steps occur when a user authenticates with a hashed password.

1. The user enters credentials such as a username and password.
2. The user’s system hashes the password and sends the hash to the authenticating system.
3. The authenticating system compares this hash to the hash stored in the password database file. If it matches, it indicates the user entered the correct password.

Birthday Attack

A *birthday attack* focuses on finding collisions. Its name comes from a statistical phenomenon known as the birthday paradox. The birthday paradox states that if there are 23 people in a room, there is a 50 percent chance that any two of them will have the same birthday. This is not the same year, but instead the same month and day, such as March 30.

Rainbow Table Attacks

It takes a long time to find a password by guessing it, hashing it, and then comparing it with a valid password hash. However, a *rainbow table* reduces this time by using large databases of precomputed hashes. Attackers guess a password (with either a dictionary or a brute-force method), hash it, and then put both the guessed password and the hash of the guessed password into the rainbow table.

Sniffer Attacks

Sniffing captures packets sent over a network with the intent of analyzing the packets. A sniffer (also called a packet analyzer or protocol analyzer) is a software application that captures traffic traveling over the network. Administrators use sniffers to analyze network traffic and troubleshoot problems.

Spoofing Attacks

Spoofing (also known as masquerading) is pretending to be something, or someone, else. There is a wide variety of spoofing attacks.

Email Spoofing Spammers commonly spoof the email address in the From field to make an email appear to come from another source.

Phone Number Spoofing Caller ID services allow users to identify the phone number of any caller.

Smartcard Attacks

Smartcards provide better authentication than passwords, especially when they’re combined with another factor of authentication such as a personal identification number (PIN). However, smartcards are also susceptible to attacks. A *side-channel attack* is a passive, noninvasive attack intended to observe the operation of a device. When the attack is successful, the attacker can learn valuable information contained within the card, such as an encryption key.

A smartcard includes a microprocessor, but it doesn’t have internal power. Instead, when a user inserts the card into the reader, the reader provides power to the card. The reader has an electromagnetic coil that excites electronics on the card. This provides enough power for the smartcard to transmit data to the reader.

Side-channel attacks analyze the information sent to the reader. Sometimes they can measure the power consumption of a chip, using a power monitoring attack or differential power analysis attack, to extract information. In a timing attack, they can monitor the processing timings to gain information based on how much time different computations require. Fault analysis attacks attempt to cause faults, such as by providing too little power to the card, to glean valuable information.

Summary of Protection Methods

- Control physical access to systems
- Control electronic access to files.
- Create a strong password policy
- Hash and salt passwords
- Use password masking
- Deploy multifactor authentication
- Use account lockout controls
- Use last logon notification
- Educate users about security

Activity: Select the Appropriate Access Control Type (Rule, Role, Attribute, etc.) for Specific Business Needs

INSTRUCTIONS

As a team, reflect upon and discuss actual business needs within your corporation.

- Each team should allow every participant to relate business needs within each company.
- Instead of contributing to or jumping to a conclusion on what solution there might be, each participant should ask deeper questions of the presenter to uncover additional insights into the environment.
- Expose assumptions by asking “why” a thing is so or to give an example of a statement shared.
- Create a business case for utilizing the previously reviewed access control methods. Use the best examples from each participant for each method.

Module 6

Accountability

Module Objectives

1. Name the significance of accountability in relationship to identification, authentication, and auditing.

Accountability

Ensuring that account management has assurance that only authorized users are accessing the system and that authorized users are using the system properly.

Module 7

Domain Review

Domain Summary

- Identity and access management (IAM) includes controls related to physical and logical access to assets along with managing an identity and access provisioning lifecycle.
- The essential elements of an access provisioning lifecycle include a full range of items under system management related to people, devices, and resources.
- Identification, authentication, and authorization ensure that the right users or accessing the system and that the correct usage of resources is happening.

Domain Review Questions

1. What are the two primary types of access control systems and what is one way that access control systems are maintained?

A. Physical and network; due diligence

B. Deterrent and corrective; due care and due diligence

C. Integrity and availability; by as much security as can be safely applied

D. Logical and physical; central administration of access control systems

Answer

The correct answer is D.

NIST SP 800-53 defines two primary access control systems: logical and physical, and both are maintained by administration and security policy. Due diligence and care are overarching organizational posture and actions that aid in avoiding the accusation of negligence and liability. Using as much security as can be safely applied is not a prudent approach to security and doesn’t answer the question. Integrity and availability are overarching tenants of information security.

Domain Review Questions

2. What actions specify enrolling and the opposite of enrolling user IDs within an organization?

A. Identity creation and disposition

B. Disposition only

C. Creation only

D. Provisioning and deprovisioning

Answer

The correct answer is D.

Identity creation is an activity that would be included in provisioning, but the only correct answer is provisioning and deprovisioning.

Domain Review Questions

3. What are the three roles within Security Assertion Markup Language (SAML)?

A. Identity provider, relying party, service provider

B. Identity provider, relying party, user

C. Identity provider, service provider, relative token

D. Attributes, principal, bindings

Answer

The correct answer is B.

Attributes and bindings are components of SAML. Relative token is a distractor. Relying party is an alternate term for a service provider.

Domain Review Questions

4. Name two roles related to Open Authorization (OAuth).

A. Resource provider, resource server
B. Resource provider, resource relying party
C. Authorization server, resource server
D. Authorization server, authorization owner

Answer

The correct answer is C.

There isn’t a resource provider owner in OAuth, but there is a resource owner and server. There is also no authorization owner.

Domain Review Questions

5. If an organization demanded that an enrolling party or claimant needed to present themselves in person at an enrolling agent to authenticate their assertion to their identity, what level of assurance would they be providing according to NIST SP 800-63-3?

A. IAL1

B. IAL 2

C. IAL 3

D. None of the above

Answer

The correct answer is B.

IAL 2 is remote or in-person authentication of an identity. IAL 1 is self-assertion. IAL 3 is assertion verified by a credential service provider.

Domain Review Questions

6. What provides assurance that a user of a system is consuming resources as intended?

A. Accountability

B. Noninterference

C. Spoliation

D. Subsystem

Answer

The correct answer is A.

Noninterference is a security model. Spoliation is the destruction, concealment, or damaging of information. Subsystems are low level systems that support operating systems.

Domain Review Questions

7. How does system account review differ from user account review?

A. User account review is connected to systems and system account review is connected to users

B. User account and system account review are the same

C. User account review targets user IDs and system account review targets built-in administrative and other non-user ID accounts

D. None of the above

Answer

The correct answer is C.

User account reviews are related to regular IDs and system account reviews are connected to administrator IDs and non-user IDs. Answer A is the inverse of the correct answer. Answers B and D are not true.

Domain Review Questions

8. Special Publications 800-53r4 defines physical access control as an automated system that manages the passage of people or assets through an opening(s) in a secure perimeter(s) based on (a)

A. Audit and assurance

B. Scoping and tailoring

C. Guidelines and tailoring

D. Set of authorization rules

Answer

The correct answer is D.

Tailoring and scoping are used to apply a set of controls within an environment that fit the internal requirement utilizing specific controls. Auditing the controls would provide assurance about the effectiveness of the controls.

Domain Review Questions

9. What is an appropriate reason to disable or revoke a user account after a review?

A. A user is voluntarily terminated from an organization

B. An account has been inactive for a period that surpasses the organizational policy

C. The user account is no longer appropriate for the job description or role

D. All of the above

Answer

The correct answer is D.

Answers A through C are all correct because these are appropriate reasons to disable or revoke a user account.

Domain Review Questions

10. Your organization shares a customer base with another organization that you partner with to provide a more complete solution. You will not be sharing the customer user IDs or passwords with your partner, so how will your partner allow your customers to access their resources in a secure fashion?

A. They will not allow it because it is not ethical

B. Your organizations will use Oauth

C. XML will solve the needs related to the requirements

D. Set up two servers and exchange information in a sanitized fashion

Answer

The only correct answer is B.

Answers A and D are illogical, incorrect, and don’t solve the requirements. XML is the underlying language used by SAML and while SAML answers to the needs for federated security, SAML wasn’t mentioned.