CompTIA Security+

5.0 Access Control and Identity Management

Objective 5.1

- Compare and Contrast the Function and Purpose of Authentication Services.

Authentication

- A mechanism by which a person proves their identity to a system.
- It's the process of proving that a subject is the valid user of an account.
- Often, a simple username and password, but other more complex authentication factors or credential-protection mechanisms are used in order to provide strong protection for the logon and account-verification process.
- The authentication process requires that the subject provide an identity and then proof of that identity.

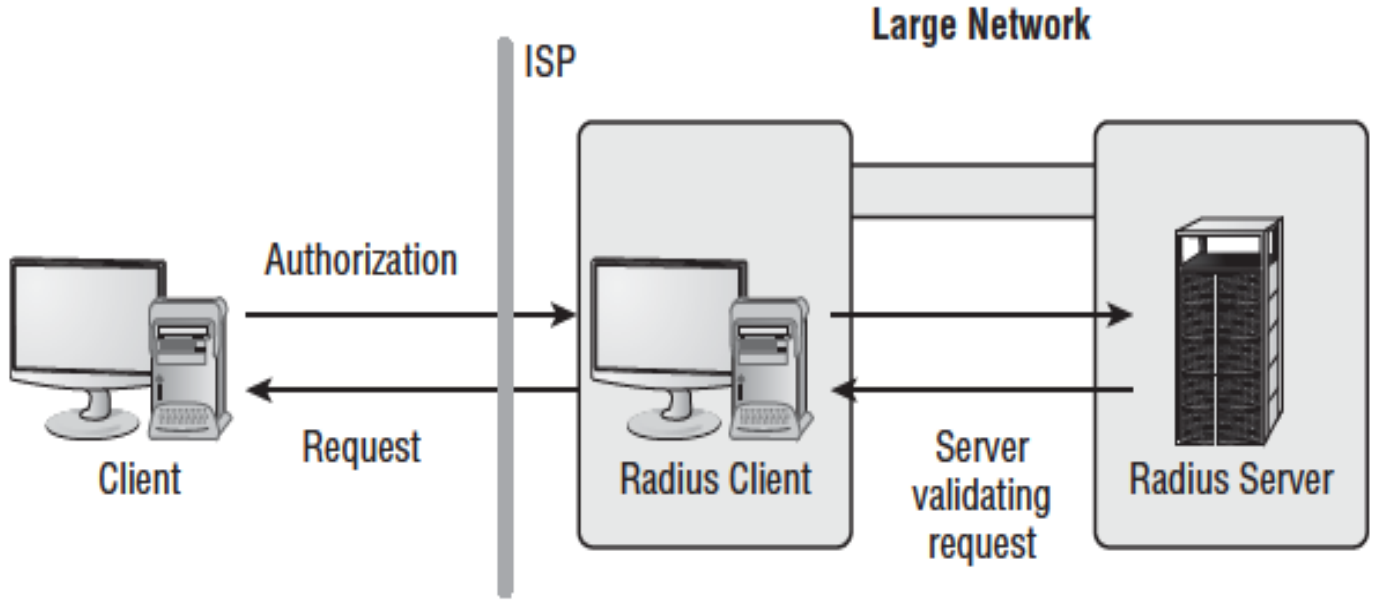
Remote Authentication Dial-In User Service (RADIUS)

- A centralized authentication system often deployed to provide an additional layer of security for a network.
- Offloads authentication of remote access clients from domain controllers or even the remote access server to a dedicated RADIUS server.
- Can be used with any type of remote access, including dial-up, virtual private network (VPN), and terminal services

- AAA server combining authentication and authorization but separates accounting, allowing less flexibility than TACACS+.
- UDP port 1812 for authentication – UDP port 1813 for accounting.

RADIUS

FIGURE 5.1 The RADIUS client manages the local connection and authenticates against a central server.



Terminal Access Controller Access Control System (TACACS)

- TACACS is another example of an AAA server similar to RADIUS.
- Uses ports TCP 49 and UDP 49.

- XTACACS was the first proprietary Cisco revision of TACACS.

- TACACS and XTACACS are utilized on many older systems but have been all but replaced by TACACS+ on current systems

Terminal Access Controller Access Control System Plus (TACACS+)

- TACACS+ was the second major revision by Cisco of this service into yet another proprietary version
- None of the three versions of TACACS are compatible with each other.
- Separates Authentication and Authorization of the AAA functions, allowing more flexibility in protocol selection
- Runs only on TCP port 49

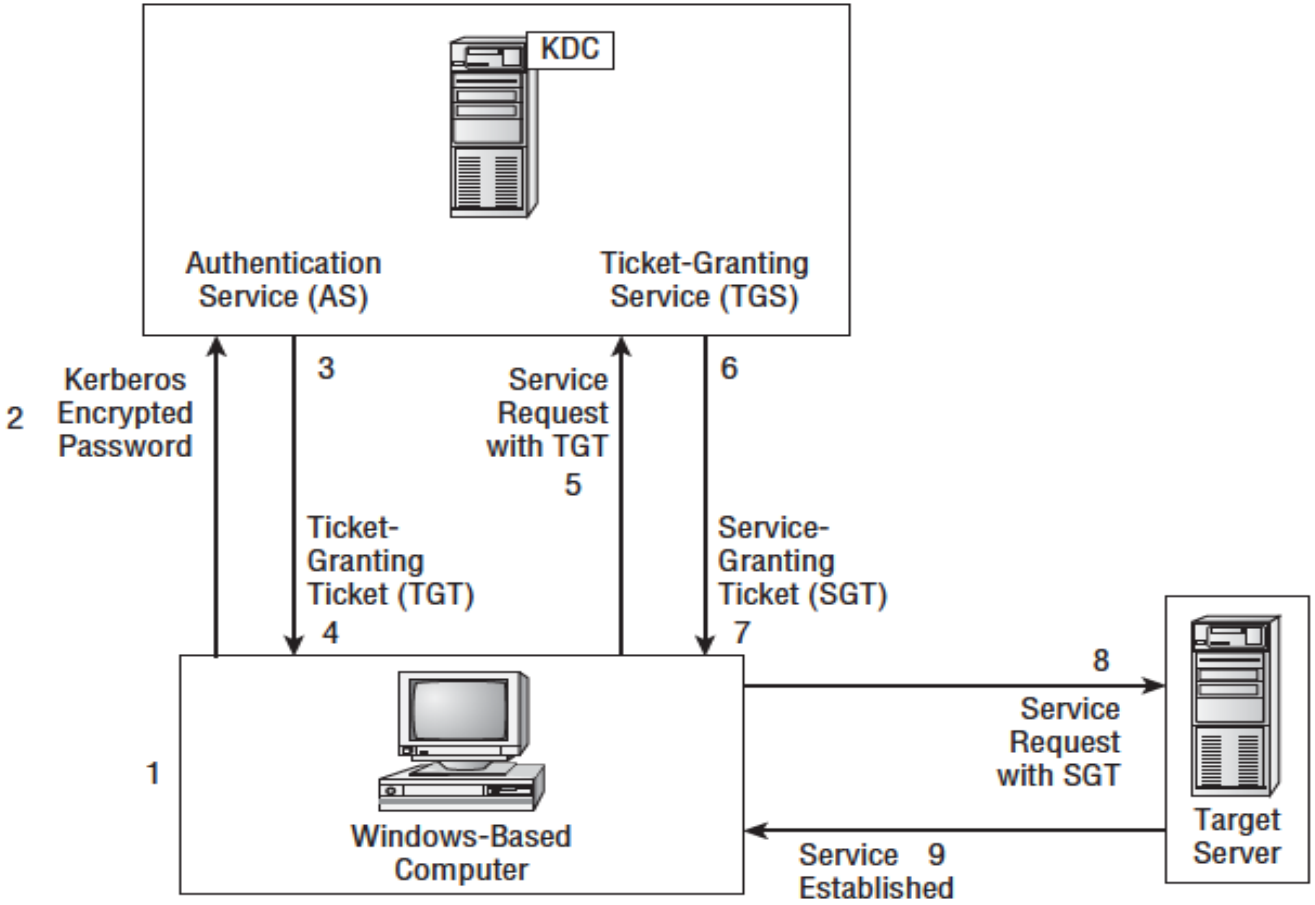
RADIUS and TACACS

Kerberos

- Based on a time-sensitive ticket granting system
- Developed by MIT to use SSO
- Can manage access control to many services using one centralized authentication server
- The Three Core Components of Kerberos:
  - Key Distribution Center (KDC)
  - Ticket-Granting Service (TGS)
  - Authentication Service (AS)

Kerberos Authentication Process

FIGURE 5.2 The Kerberos authentication process



Kerberos

Mutual Authentication

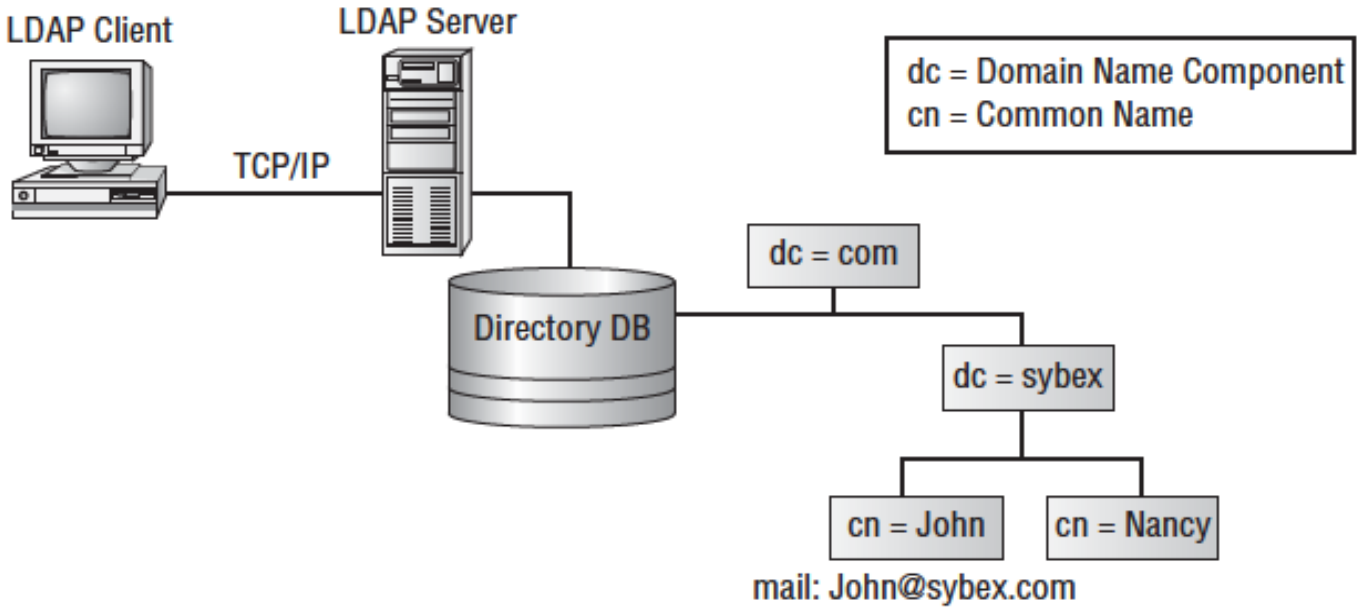
•Mutual Authentication, also called two-way authentication, Is a process or technology in which both entities in a communications like authenticate each other.

•You authenticate the server and the server authenticates you

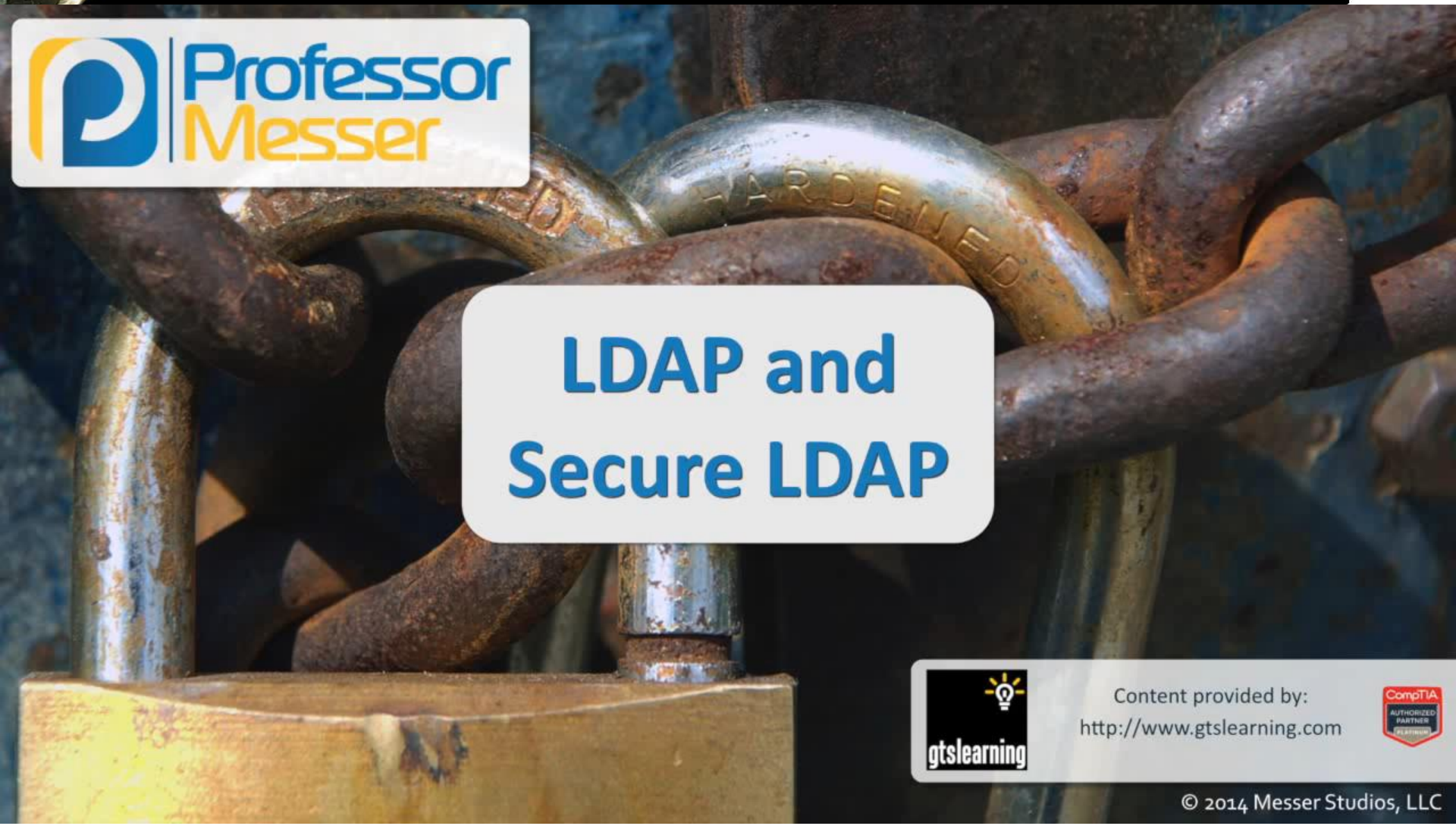
Lightweight Directory Access Protocol (LDAP)

A directory service is a managed list of network resources. Through the use of a directory services, large networks are easier to navigate, manage, and secure. Ports 389 (LDAP) and 636 (LDAP over SSL)

FIGURE 5.3 An example of an LDAP-based directory services structure



LDAP and Secure LDAP



Security Assertion Markup Language (SAML)

- SAML is an open-standard data format based on XML for the purpose of supporting the exchange of authentication and authorization details between systems, services, and devices.

- SAML was designed to address the difficulties related to the implementation of **single sign-on (SSO) over the Web**.

- SAML's solution is based on a trusted third-party mechanism where the subject or user (the principle) is verified through a trusted authentication service (the identity provider) in order for the target server or resource host (the service provider) to accept the identity of the visitor

Security Assertion Markup Language (SAML)

Student Check

Which of the following technologies can be used to add an additional layer of protection between a directory services–based network and remote clients?

- ❍ A. SMTP
- ❍ B. RADIUS
- ❍ C. PGP
- ❍ D. VLAN

Student Check

Which of the following technologies can be used to add an additional layer of protection between a directory services–based network and remote clients?

- ❍ A. SMTP
- ❍ B. RADIUS
- ❍ C. PGP
- ❍ D. VLAN

Student Check

Kerberos is used to perform what security service?

- ❍ A. Authentication protection
- ❍ B. File encryption
- ❍ C. Secure communications
- ❍ D. Protected data transfer

Student Check

Kerberos is used to perform what security service?

- A. Authentication protection
- B. File encryption
- C. Secure communications
- D. Protected data transfer

Student Check

LDAP operates over what TCP ports?

- ❍ A. 636 and 389
- ❍ B. 110 and 25
- ❍ C. 443 and 80
- ❍ D. 20 and 21

Student Check

LDAP operates over what TCP ports?

- A. 636 and 389
- B. 110 and 25
- C. 443 and 80
- D. 20 and 21

Student Check

What mechanism is used to support the exchange of authentication and authorization details between systems, services, and devices?

- ❍ A. Biometric
- ❍ B. Two-factor authentication
- ❍ C. SAML
- ❍ D. LDAP

Student Check

What mechanism is used to support the exchange of authentication and authorization details between systems, services, and devices?

- ❍ A. Biometric
- ❍ B. Two-factor authentication
- ❍ C. SAML
- ❍ D. LDAP

Student Check

Which of the following services provides the capability of endpoint validation for both client and server?

- ❍ A. LDAP
- ❍ B. Kerberos
- ❍ C. RADIUS
- ❍ D. XTACACS

Student Check

Which of the following services provides the capability of endpoint validation for both client and server?

- ❍ A. LDAP
- ❍ B. Kerberos
- ❍ C. RADIUS
- ❍ D. XTACACS

Student Check

Which of the following services are used to provide authentication, authorization, and auditing of access requests? (Select all answers that apply.)

- ❍ A. TACACS+
- ❍ B. TACACS
- ❍ C. IEEE 802.1x
- ❍ D. RADIUS

Student Check

Which of the following services are used to provide authentication, authorization, and auditing of access requests? (Select all answers that apply.)

- ❍ A. TACACS+
- ❍ B. TACACS
- ❍ C. IEEE 802.1x
- ❍ D. RADIUS

Objective 5.2

Explain the fundamental concepts and best practices related to authentication, authorization and access control

Authentication, Authorization, Access Control

- ***Authentication*** is proving your identity to a system to validate that a user is who they say they are and correlates with the act of logging on.

- ***Access Control*** – The mechanism by which users are granted or denied the ability to interact with and use resources. Often referred to using the term **Authorization**.

- ***Authorization*** – defines the type of access to resources that users are granted or what users are authorized to do. Often considered the next logical step immediately after Authentication.

With proper authorization or access control, a system can properly control access to resources in order to prevent unauthorized access.

Identification vs. Authentication vs. Authorization

It's important to understand the differences among identification, authentication, and authorization.

Identification and authentication are commonly used as a two-step process, but they're distinct activities.

- **Identification***:* is the claiming of an identity. A network element goes through a process to recognize a valid users identity. (Username)
- **Authentication**: is the act of verifying or proving the claimed identity.
- **Authorization**: is the mechanism that controls what a subject can and can't do. Authorization is commonly called access control or access restriction.

Access Control Best Practices

- Implicit deny
- Least privilege
- Separation of duties
- Expiration (Accounts/Passwords)
- Job Rotations
- Time of day restrictions

Mandatory Access Control (MAC)

- The most basic form of access control involves the assignment of labels to resources and accounts

- Examples include SENSITIVE, SECRET, and PUBLIC
  Most restrictive
- If the labels on the account and resource do not match, the resource remains unavailable in a nondiscretionary manner

- Often used within governmental systems where resources and access may be granted based on categorical assignment such as classified, secret, or top secret

- Applies to all resources within the network and does not allow users to extend access rights by proxy

Discretionary Access Control (DAC)

- Slightly more complex system of access control involves the restriction of access for each resource in a discretionary manner

- Access rights are configured at the discretion of accounts with authority over each resource including the ability to extend administrative rights through the same mechanism

- **The owner assigns security levels based on objects and subjects and can make his own data available to others at will**

Rule-Based Access Control (RBAC)

- Non-discretionary technique that is based on a set of operational rules and restrictions
- Rule sets are always examined before a subject is given access to objects
- Think Access Control Lists (ACL)
  - Security Group in AD

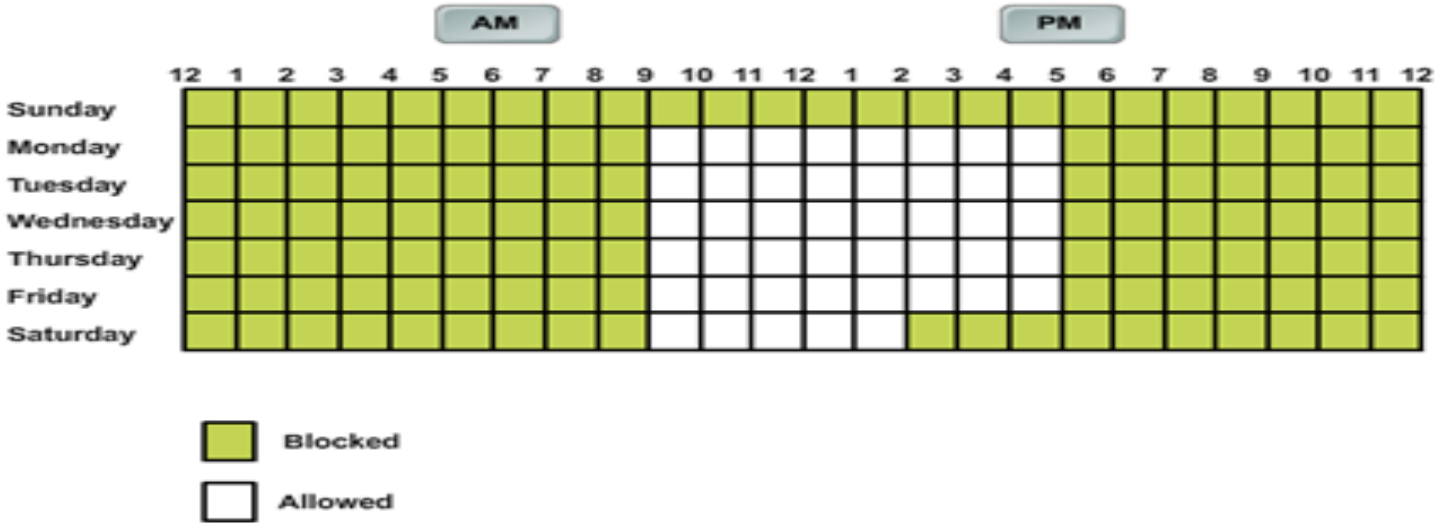
Role-Based Access Control (RBAC)

- Access rights are first assigned to roles and accounts are then associated with these roles without direct assignment of resource access rights
- Provides the greatest level of scalability within large enterprise scenarios
- Can be implemented as MAC or DAC
- Based on job

Time of Day Restrictions

Restrictions for multiple accounts on an account by account basis can be cumbersome in an enterprise environment; so an Administrator can apply Time of Day Restrictions to specific groups of users in the organization through Group Policy.

The group policy configuration for the Time of Day restrictions will specify the time period of allowed or blocked Access to enterprise resources.



*Authentication Factors

- Something you know or Type 1 Factor

(such as a password, code, PIN, combination, or secret phrase)

- Something you have or Type 2 Factor

(such as a smart card, token device, or key)

- Something you are or Type 3 Factor

(such as a fingerprint, a retina scan, or voice recognition; often referred to as *biometrics*)

- Somewhere you are

(such as a physical or logical location)

- Something you do

(such as your typing rhythm, a secret handshake, or a private knock)

(Note: The factors of **somewhere you** are and **something you do** are not given Type labels.)

Something You Know (Type 1 Factor)

The idea here is that you know a secret, often called a ***PASSWORD*** that nobody else does. Thus, knowledge of a secret distinguishes you from all other individuals. And the authentication system simply needs to check to see if the person claiming to be you knows the secret.

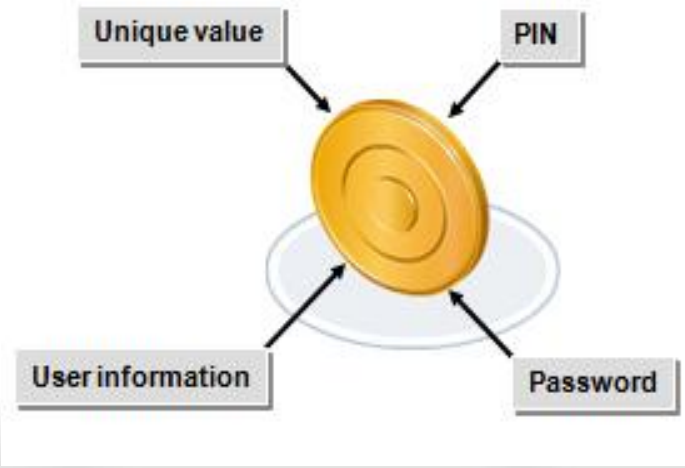
Unfortunately, use of secrets is not the best solution. If the secret is entered at some sort of keyboard, an eavesdropper ("shoulder surfing") might see the secret being typed.

Something you have (Type 2 Factor)

- **Token** – usually a hardware device, but it can be implemented in software as a logical token used to generate temporary single-use passwords for the purpose of creating stronger authentication.

- Other Authentication factors that are something you have can be devices such as smart cards (CAC)/(PIV), ID badges, or data packets, that store authentication information

- Can store PINs, information about users, and/or passwords



Something you are (Type 3 Factor)

Biometrics – the collection of physical attributes of the human body that can be used as an identification or an authentication factor.

Authentication based on "something you are" will employ behavioral and physiological characteristics of the user and must be easily measured accurately and preferably are things that are difficult to spoof.

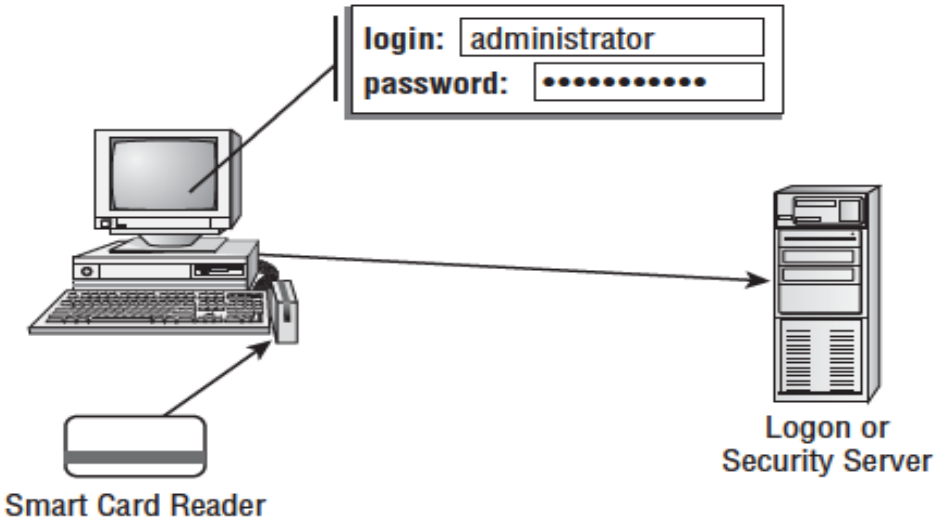
- Retinal scan – pattern of the back of the eye
- Iris scan – the color part of the front of the eye
- Fingerprint reader
- Handprint reader
- Voice print
- Keystroke timing
- Signature

The characteristic is measured and compared with what has been stored.

Multifactor Authentication

Requirement that a user must provide two or more authentication factors in order to prove their identity. There are three generally recognized categories of authentication factors.

FIGURE 5.5 Two-factor authentication



TOTP / HOTP

Time-based one-time password (TOTP) tokens or synchronous dynamic password tokens are devices or applications that generate passwords at fixed time intervals, such as every 60 seconds.

HMAC-based one-time password (HOTP) tokens or asynchronous dynamic password tokens are devices or applications that generate passwords not based on fixed time intervals but instead based on a non-repeating one-way function, such as a hash or hash message authentication code.

Off-by-One Problem – the non-time-based seed or key synchronization gets desynchronized, the client may be calculating a value that the server has already tossed or has not yet generated

Both use password shown on the token + a PIN or passphrase for multifactor authentication

CHAP / PAP

Challenge Handshake Authentication Protocol (CHAP) is a means of authentication based on a random challenge number combined with the password hash to compute a response.

Password Authentication Protocol (PAP) in an unsecure plaintext password-logon mechanism.

Single Sign-on (SSO)

A relationship between the client and the network wherein the client is allowed to log on one time, and all resource access is based on that logon

Privilege Management

Privilege Management: augments Identification and Authentication Services by facilitation registered identity services that can grant access to resources based on a defined user account, group, or role used in an organization. The defined user account, group, or roles can correspond directly to the Access-Control methodologies DAC, MAC, and RBAC.

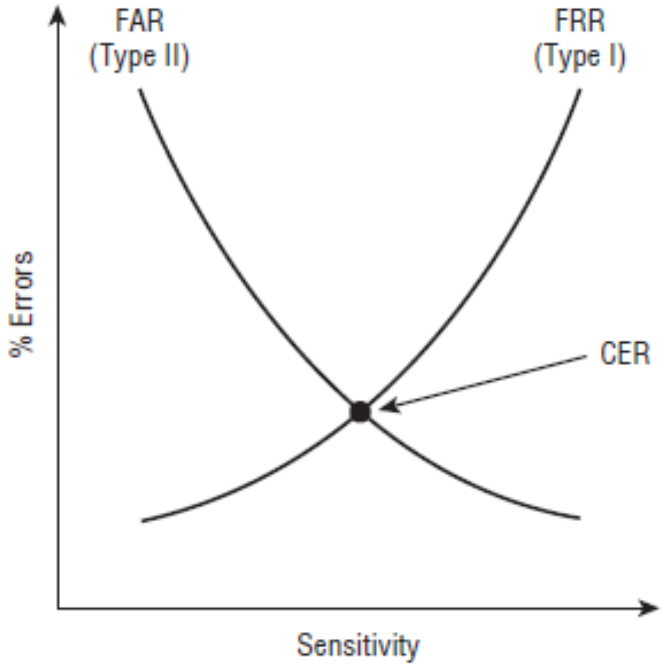
FRR/FAR/CER

An exact match is not expected, nor should it be because of error rates associated with biometric sensors. (For example, fingerprint readers today normally exhibit error rates upwards of 5%.)

False Rejection Rate (FRR or Type I) errors
Number of failed authentications for valid subjects based on device sensitivity

False Acceptance Rate (FAR or Type II) errors
Number of accepted invalid subjects based on device sensitivity.

These two error measurements can be mapped on a graph comparing sensitivity level versus rate of errors. The point on this graph where these two rates intersect is known as the **Crossover Error Rate (CER)**



None Type Authentication Factors

- **Somewhere you are**:

  A location-based verification. Examples include a physical location or a logical address, such as domain name, an IP address, or a MAC address. See the earlier

- **Something you do**:

  Involves some skill or action you can perform. Examples include your typing rhythm, a secret handshake, or a private knock.

Federation

- **Federation or federated identity** is a means of linking a subject's accounts from several sites, services, or entities in a single account
- Web-based Single Sign-on.
- Often implement trans-site authentication using SAML

Student Check

If you have a smart card that contains details of your iris coloring and retinal patterns, which two types of authentication would be involved in a successful access request?

- ❍ A. What you have and what you do
- ❍ B. What you do and what you are
- ❍ C. What you are and what you know
- ❍ D. What you have and what you are

Student Check

If you have a smart card that contains details of your iris coloring and retinal patterns, which two types of authentication would be involved in a successful access request?

- ❍ A. What you have and what you do
- ❍ B. What you do and what you are
- ❍ C. What you are and what you know
- ❍ D. What you have and what you are

Student Check

Which biometric measure involves scanning the back of the eye?

- ❍ A. Retina
- ❍ B. Iris
- ❍ C. Facial recognition
- ❍ D. Signature

Student Check

Which biometric measure involves scanning the back of the eye?

- A. Retina
- B. Iris
- C. Facial recognition
- D. Signature

Student Check

Which of the following are standard forms of access control? (Select all correct answers.)

- ❍ A. DAC
- ❍ B. MAC
- ❍ C. RBAC
- ❍ D. TCSEC

Student Check

Which of the following are standard forms of access control? (Select all correct answers.)

- ❍ A. DAC
- ❍ B. MAC
- ❍ C. RBAC
- ❍ D. TCSEC

Student Check

What method of access control is best suited for environments with a high rate of employee turnover?

- ❍ A. MAC
- ❍ B. DAC
- ❍ C. RBAC
- ❍ D. ACL

Student Check

What method of access control is best suited for environments with a high rate of employee turnover?

- ❍ A. MAC
- ❍ B. DAC
- ❍ C. RBAC
- ❍ D. ACL

Student Check

In a MAC environment, when a user has clearance for assets but is still unable to access those assets, what other security feature is in force?

- ❍ A. Principle of least privilege
- ❍ B. Need to know
- ❍ C. Privacy
- ❍ D. Service-level agreement

Student Check

In a MAC environment, when a user has clearance for assets but is still unable to access those assets, what other security feature is in force?

- ❍ A. Principle of least privilege
- ❍ B. Need to know
- ❍ C. Privacy
- ❍ D. Service-level agreement

Student Check

Which of the following is not a benefit of single sign-on?

- ❍ A. The ability to browse multiple systems
- ❍ B. Fewer usernames and passwords to memorize
- ❍ C. More granular access control
- ❍ D. Stronger passwords

Student Check

Which of the following is not a benefit of single sign-on?

- ❍ A. The ability to browse multiple systems
- ❍ B. Fewer usernames and passwords to memorize
- ❍ C. More granular access control
- ❍ D. Stronger passwords

Student Check

Federation is a means to accomplish _____.

- ❍ A. Accountability logging
- ❍ B. ACL verification
- ❍ C. Single sign-on
- ❍ D. Trusted OS hardening

Student Check

Federation is a means to accomplish _____.

- ❍ A. Accountability logging
- ❍ B. ACL verification
- ❍ C. Single sign-on
- ❍ D. Trusted OS hardening

Student Check

Which of the following is an example of a Type 2 authentication factor?

❍ A. Something you have, such as a smart card, an ATM card, a token device, or a memory card

❍ B. Something you are, such as fingerprints, voice print, retina pattern, iris pattern, face shape, palm topology, or hand geometry

❍ C. Something you do, such as type a passphrase, sign your name, or speak a sentence

❍ D. Something you know, such as a password, personal identification number (PIN), lock combination, passphrase, mother's maiden name, or favorite color

Student Check

Which of the following is an example of a Type 2 authentication factor?

❍ A. Something you have, such as a smart card, an ATM card, a token device, or a memory card

❍ B. Something you are, such as fingerprints, voice print, retina pattern, iris pattern, face shape, palm topology, or hand geometry

❍ C. Something you do, such as type a passphrase, sign your name, or speak a sentence

❍ D. Something you know, such as a password, personal identification number (PIN), lock combination, passphrase, mother's maiden name, or favorite color

Objective 5.3

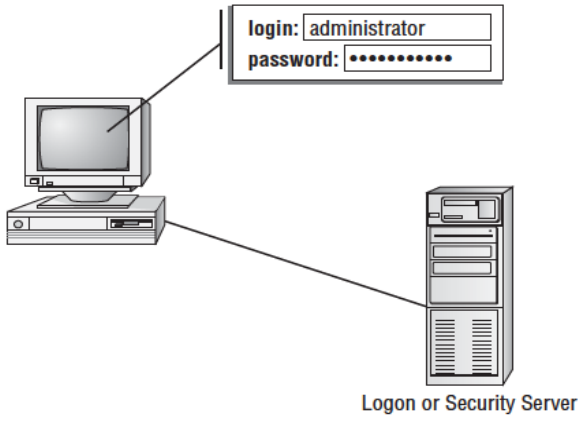
The combination of a username and a password is the most common form of authentication.

If the provided password matches the password stored in a system's accounts database for the specified user, then that user is authenticated to the system.

Just because using a username and password is the most common form of authentication, that doesn't mean it's the most secure.

It generally considered to be the least secure form of authentication.

FIGURE 5.7 A basic logon process employing a username and password



Account Policy Enforcement

Account Policy Enforcement:

Strong passwords consist of

- Numerous characters (16 or more)
- At least three types of characters (uppercase and lowercase letters, numerals, and keyboard symbols)
- Changed on a regular basis (every 90 days)
- Don't include any dictionary or common words or acronyms
- Don't include any part of the subject's real name, username, or email address.

These features can be implemented as a requirement through **account policy enforcement**.

This is the collection of password requirement features in the OS, often called a **password policy**.

Passwords should be strong enough to resist discovery through attack but easy enough for the person to remember. This can sometimes be a difficult line to walk. Training users on picking strong passphrases and memorizing them is an important element of modifying risky behavior.

Credential Management

A service or software product designed to store, manage, and even track user credentials.

Many credential-management options are available for enterprise networks, where hundreds or thousands of users must be managed. However, most credential-management solutions are designed for end-user deployment.

Credential management products allow a person to store all their online (and even local) credentials in a local or cloud-based secured digital container.

Examples of products of this type include LastPass, 1Password, KeePass 2, and Dashlane.

By using a credential manager, users can define longer and more random credentials for their various accounts without the burden of having to remember them or the problem of writing them down.

Group Policy

The mechanism by which Windows systems can be managed in a Windows network domain environment.

Group Policy Object (GPO) – a collection of registry settings that can be applied to a system at the time of boot up or at the moment of user login.

Group policy enables a Windows administrator to maintain consistent configurations and security settings across all members of a large network.

In the vast array of setting options available in a GPO, there are numerous settings related to credentials, such as password complexity requirements, password history, password length, account lockout settings, and so on.

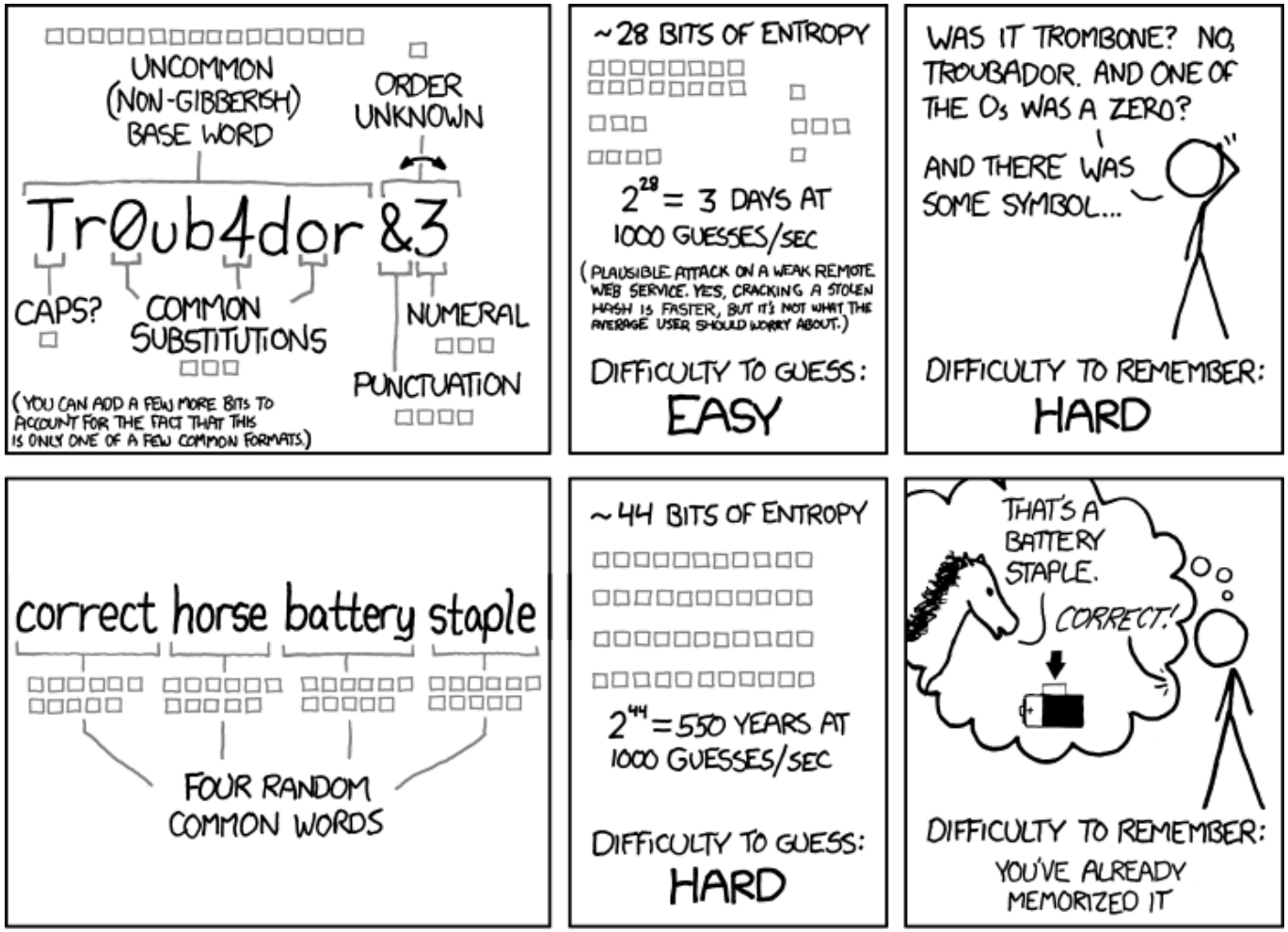
Password Expiration and Recovery

- All password should expire
  - 30, 60, 90 days
  - Password History Policy
- Critical systems might change more frequently
- Should have a formal process for password recovery
  - Should be in-person

Exam Alert

- User is added to multiple Groups, the user will have the most restrictive access of the Groups
- User is added to a Group with liberal access and a Group with no access
- This results in the user having NO Access

Password Complexity and Length



Password Complexity and Length

- The password policy typically comprised of:
  - Minimum password length
  - Maximum password age
  - Minimum password age
  - Password history retention
  - Complexity requirement

- 8 characters – Strong
- Over 12 characters – Fairly Secure
- Over 15 characters – Very Secure

Account Lockout and Disablement

- Too many bad passwords will cause lock-out
- Disable accounts when users leave organizations
  - Be careful with deletions-encryption keys

User Assigned vs. Group-Based Privileges

- User assigned
  - Individual user are granted specific rights
  - Doesn't scale well

- Group-based
  - Put many users into one group
  - Set privileges for the group
  - Add remove users to the groups
  - Users can be members of multiple groups

Student Check

Which type of password policy will protect against reuse of the same password over and over again?

- ❍ A. Account lock-out
- ❍ B. Password complexity
- ❍ C. Expiration
- ❍ D. Password history

Student Check

Which type of password policy will protect against reuse of the same password over and over again?

- ❍ A. Account lock-out
- ❍ B. Password complexity
- ❍ C. Expiration
- ❍ D. Password history

Student Check

Which is the strongest form of password?

- ❍ A. More than eight characters
- ❍ B. One-time use
- ❍ C. Static
- ❍ D. Different types of keyboard characters

Student Check

Which is the strongest form of password?

- A. More than eight characters
- B. One-time use
- C. Static
- D. Different types of keyboard characters