Identity and Access Management

4.0 Identity and Access Management

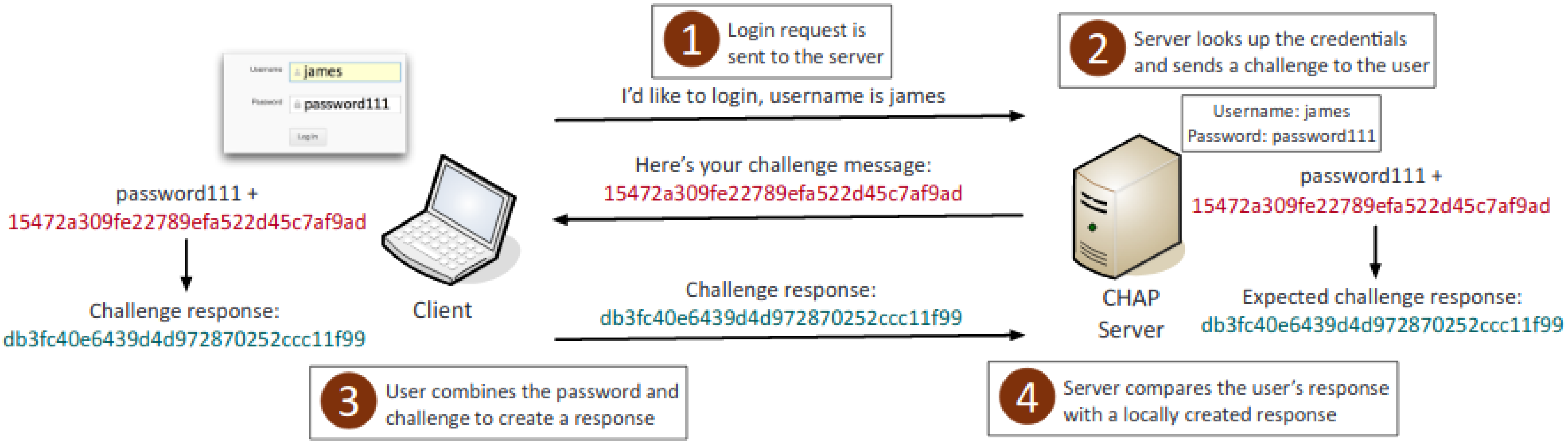
4.1 Compare and contrast identity and access management concepts

1. Identification, authentication, authorization and accounting (AAA):
    1. **Identification**: Finding the unique individual on the system.
    2. **Authentication**: The ability to tell if an individual is actually who they claim they are.
    3. **Authorization**: Determining what an individual can and cannot access on a system.
    4. **Accounting**: The tracking of an individual's actions on the system.
2. Multifactor authentication: Uses at least two of the factors of authentication.
    1. **Something you are** (biometric auth, difficult to change)
    2. **Something you have** (smart card, usb token, phone…)
    3. **Something you know** (password, pin, pattern…)
    4. **Somewhere you are** (location, IP, geolocation area…)
    5. **Something you do** (handwriting, typing technique, biometrics)
3. **Federation**: The authenticating and authorizing between two parties. Ex. Logging onto Facebook with Google account.
4. **Single sign-on**: Only uses one of the factors of authentication.
5. **Transitive trust**: There are more than two entities, one entity is trusted because they are trusted by someone the company trusts.

4.2 Given a scenario, install and configure identity and access services.

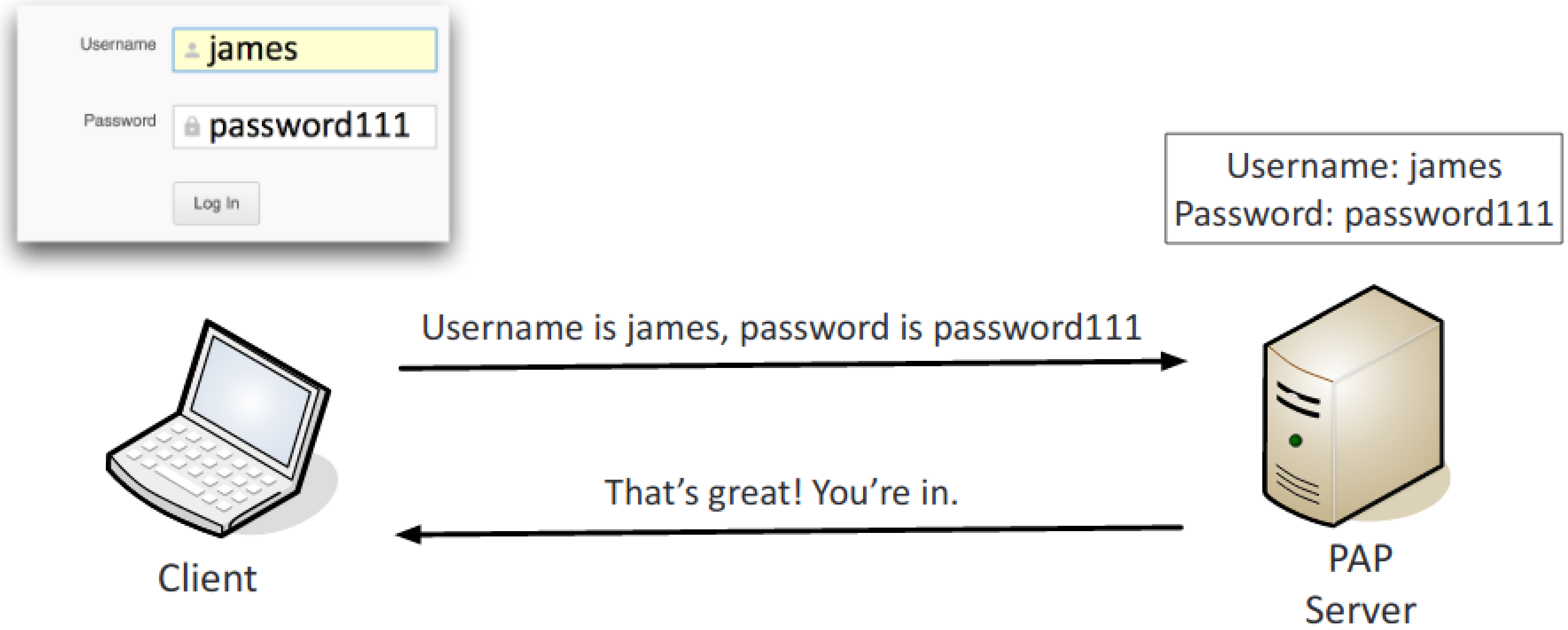
1. **LDAP** (Lightweight Directory Access Protocol): Queries information about the directory. Is a hierarchical structure; CN = Common Name, OU = Organizational Unit, DC = Domain Controller. Utilizes TCP/IP, TCP/UDP ports 389.
2. **Secure LDAP**: LDAP over SSL/TLS, uses TCP on port 636. Does not send queries in plain text.
3. **Kerberos**: Developed by MIT, for mutual authorization between client and server. It uses a ticket granting system for authorization. Is a government standard.
4. **TACACS+** (Terminal Access Controller Access Control System): Runs TCP over port 49, encrypts all parts of communication. Does not suffer due to security issues caused by RADIUS. Authorization and Authentication are separated for granular control.

5. **CHAP** (Challenge Handshake Authentication Protocol): Authenticates PPP clients to the server. Uses a one-way hash based on a shared secret that is compared on the client and server end. Does not send plaintext over the wire.



Username james
Password password111
Login
1 Login request is sent to the server
I'd like to login, username is james
2 Server looks up the credentials and sends a challenge to the user
Username: james
Password: password111
password111 +
15472a309fe22789efa522d45c7af9ad
Challenge response:
db3fc40e6439d4d972870252ccc11f99
Client
Here's your challenge message:
15472a309fe22789efa522d45c7af9ad
Challenge response:
db3fc40e6439d4d972870252ccc11f99
CHAP Server
password111 +
15472a309fe22789efa522d45c7af9ad
Expected challenge response:
db3fc40e6439d4d972870252ccc11f99
3 User combines the password and challenge to create a response
4 Server compares the user's response with a locally created response

6. **PAP** (Password Authentication Protocol): Username and password are sent as plaintext and are no longer used.



7. **MS-CHAP** (Microsoft CHAP): Delivers a two-way, mutual authentication between the server and client. Separate keys are created for sent and received data. Is seen as weak due to it using a 5-bit encryption system, same as NTLM.

8. **RADIUS** (Remote Authentication and Dial-in User service): Combines authentication and authorization, only encrypts the passwords, each network device must contain an authorization configuration. There is no command logging, and minimal vendor support. Uses ports 1812 for authentication and authorization and port 1813 for accounting functions.
9. **SAML** (Security Association Markup Language): Authenticates through a third-party source to gain access, the resource is not responsible for the authentication. The request is passed through a trusted third-party server.
    1. The three roles are: Principle (the user or client), identity provider (the one who assures the identity of the principle), and service provider (a web service of some type.)
10. **OpenID Connect**: OpenID Connect handles the authentication part of the identification process and uses OAuth for authorization.
11. **OAUTH** (Open Standard for Authorization): Token authorization happens in the background. Uses a logon from a larger trusted service.
12. **Shibboleth**: An open-source software that uses SAML to provide a third-party federated SSO authentication.
13. **Secure token**: An authentication mechanism that can be used to identify and authenticate, and to deny and allow access.
14. **NTLM** (New Technology LAN Manager): Used for authenticating in a Windows domain, was replaced by Kerberos for the most part.
    1. NTMLv2: Is the most common form used, is somewhat insecure.

4.3 Given a scenario, implement identity and access management controls.

1. Access control models:
    1. **MAC** (Mandatory Access Control): Based on classification rules. Objects are given sensitivity labels, subjects given clearance labels, and users obtain access by having the correct clearance. The classifications are hierarchical.
    2. **DAC** (Discretionary Access Control): Is based on user identity. Users are granted access through ACLs placed on objects through the object's owner or creator.
    3. **ACL** (Access Control List): A security logical device attached to all objects and resources, it defines which users are granted or denied access.
    4. **ABAC** (Attribute Based Access Control): Assigning access and privileges through a scheme of attributes. Relations and criteria determine access; time of day, location, and/or IP address.
    5. **Role-based access control**: Access is based on the job and position of the user. Changing permissions of a group changes the permissions for all of the members. Not good for companies with high turn-over rates.
    6. **Rule-based access control**: Rules are created by the admin to monitor usage and if a user needs access they must meet the requirements of the rules. Rules are enforced regardless of the user.
2. Physical access control:
    1. **Proximity cards**: A smart card that does not require direct contact.
    2. **Smart cards**: Cards that contain identification/authentication information in an integrated circuit chip. Often uses dual factor authentication; something you have (the card), and something you know (a pin or password).
3. Biometric factors: Verifies identity through physical features.
    1. **Fingerprint scanner**: Scans the unique patterns of the fingerprint to grant access.
    2. **Retinal scanner**: Blood vessels in the back of the retina.
    3. **Iris scanner**: Scans the Iris.
    4. **Voice recognition**: The identification and translation of spoken language for authorization of a user. Is vulnerable to impersonation.
    5. **Facial recognition**: The identification of an individual from a digital image or a video frame. Is vulnerable to impersonation.

    6. **False acceptance rate** (FAR): Incorrectly identifies an unauthorized user as an authorized user. Type 2 error.
    7. **False rejection rate** (FRR): Incorrectly identifies an authorized user as an unauthorized user. Type 1 error.
    8. **Crossover error rate** (CER): The point on a graph where the FAR and FRR meet. The lowest CER point is the most accurate biometric device for a body part.
4. **Tokens**
    1. **Hardware**: A device that displays and constantly generates a pin or password.
    2. **Software**: An app or software that generates a token.
    3. **HOTP/TOTP**: Open source standards to generate one-time use passwords.
        1. HOTP (HMAC-based One-Time Password): Can be used only once before it expires.
        2. TOTP (Time-based One-time Password): Only last for around 30 seconds before it expires.
5. **Certificate-based authentication**:
    1. **PIV/CAC/smart card**: Cards that have embedded certificates and a photo ID for authorization. The US DOD uses CAC/PIV.
    2. **PIV** (Personal identity verification): Is for civilians working for the federal government.
    3. **CAC** (Common access card): Is for Department of Defense members.
    4. **IEEE 802.1x**: Offers port-based authentication to wireless and wired networks to prevent rogue devices from connecting to secured ports.
6. **File system security**: The means of ensuring that files are encrypted and can only be used by properly authorized users have access to them or modify them.
7. **Database security**: MS and Oracle allow for the DB to be encrypted.

4.4 Given a scenario, differentiate common account management practices.

1. Account types:
    1. **User account**: An account that is a collection of information that identifies an individual and grants them specific areas of the network or system.
    2. **Shared and generic**: Multiple individuals sign into a single account. No workplace should have these, cannot distinguish the actions of the user.
2. Accounts/credentials:
    1. **Guest accounts**: An anonymous shared logon account.
    2. **Service accounts**: Performs specific maintenance actions, such as a backup, account and server operators.
    3. **Privileged accounts**: Access is set to access rights, generally referred to as system or network administrative accounts.
3. General Concepts:
    1. **Least privilege**: Rights and permission are set to bare minimum.
    2. Onboarding/offboarding:
        1. **Onboarding**: Helps new employees learn all of the facets of their new job.
        2. **Offboarding**: Helps leaving employees learn how to properly leave and potentially return to the company.
    3. **Permission auditing and review**: Looks at the rights and perms assigned to users and helps ensure the principle of least privilege is enabled.
    4. **Usage auditing and review**: Logging information on what users do.
    5. **Time-of-day restrictions**: Certain privileges are permitted or restricted based on the time of day.

6. **Recertification**: The action of regaining a certification due to the certification being expired.
7. **Standard naming convention**: Allows for the easier identification of resource location and purpose. Reduces the amount of time needed for troubleshooting and training.
8. **Account maintenance**: Making sure that accounts have the proper privileges, and unused accounts are deleted. Generally done through scripts to save time and money.
9. **Group-based access control**: Every user in a group has the same privileges.
10. **Location-based policies**: Grants and denies access based on the user's location.

4. Account policy enforcement:
   1. **Credential management**: Stores, manages, and tracks user credentials.
   2. **Group policy**: Sets different privileges of the system and allows for these to be managed or set those across entire groups or even through the entire network and every computer within it.
   3. **Password complexity**: The enforcing of complex and difficult to guess passwords.
   4. **Expiration**: The amount of time that passes before a password is required to be changed.
   5. **Recovery**: The ability to find lost passwords and usernames in case an employee forgets them.
   6. **Disablement**: Disabling an account.
   7. **Lockout**: Prevents login from specific individual after a set of failed login attempts, for a set period of time.
   8. **Password history**: Remembers past passwords and prevents the reuse of passwords.
   9. **Password reuse**: The ability to ever use the same password again.
   10. **Password length**: The minimum amount of characters that can be used in a password.
   11. **Password age**: A policy that sets how long a user can have a password before they are forced to change it.