CSF3404 Cyber Security

Chapter 6
Implementing Access Control Authentication and Account Management

Lecturer:
Waheed Ghanem
Fakhrul Adli bin Mohd Zaki
Aalim Rozli
Faculty of Ocean Engineering Technology and Informatics,
Universiti Malaysia Terengganu

Lesson Objectives

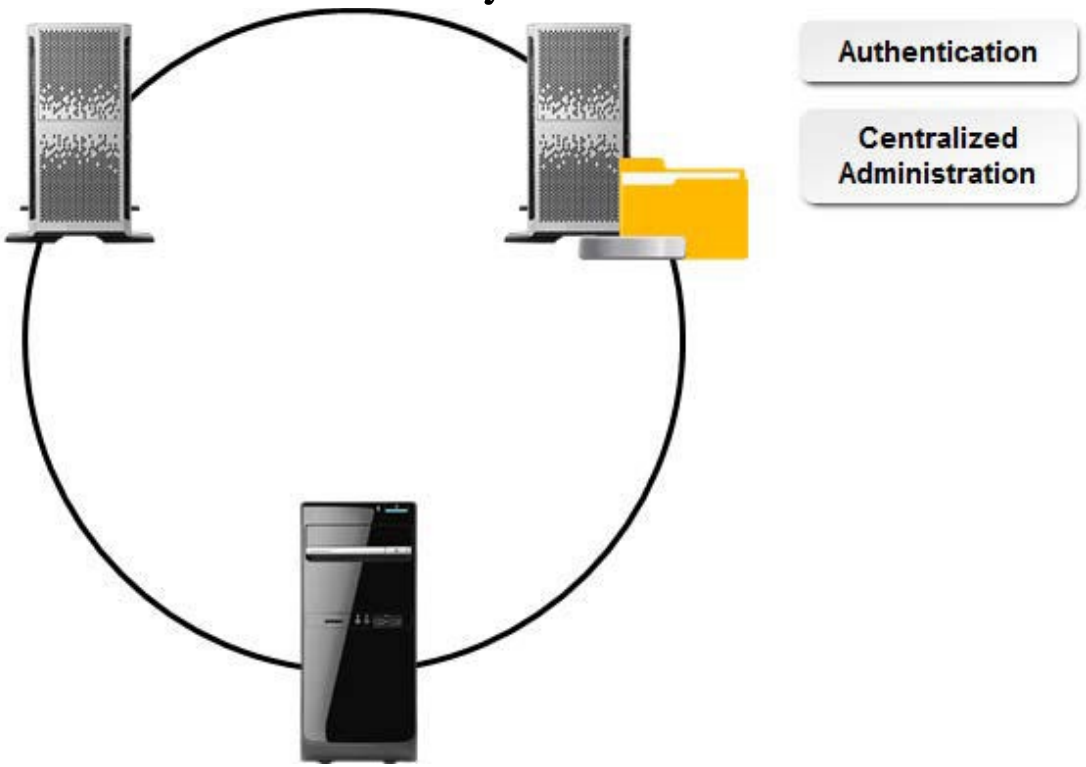
- Implement **access control** and common **authentication services**.
- Implement **account management security controls**.
- In this lesson,
  - You will identify
    - How access control methods, authentication services, and account management security measures.

Access Control and Authentication Services

- Access control and authentication are among the **primary factors** in computer security.
- **Strong** authentication and access control are the **first lines of defense** in the battle to secure network resources.
- Applying access control and authentication is not a **single process**.
- There are many different **methods** and **mechanisms**, some of which can even be combined into more complex schemes.
    - You will need to be familiar with the major access control and authentication services.

Directory Services

- A directory service is a network service that stores identity information about all the objects in a particular network, including users, groups, servers, clients, printers, and network services.
- The directory also provides **user access control** to directory objects and network resources.
- Directory services can also be used to **centralize security** and to control access to individual network resources.



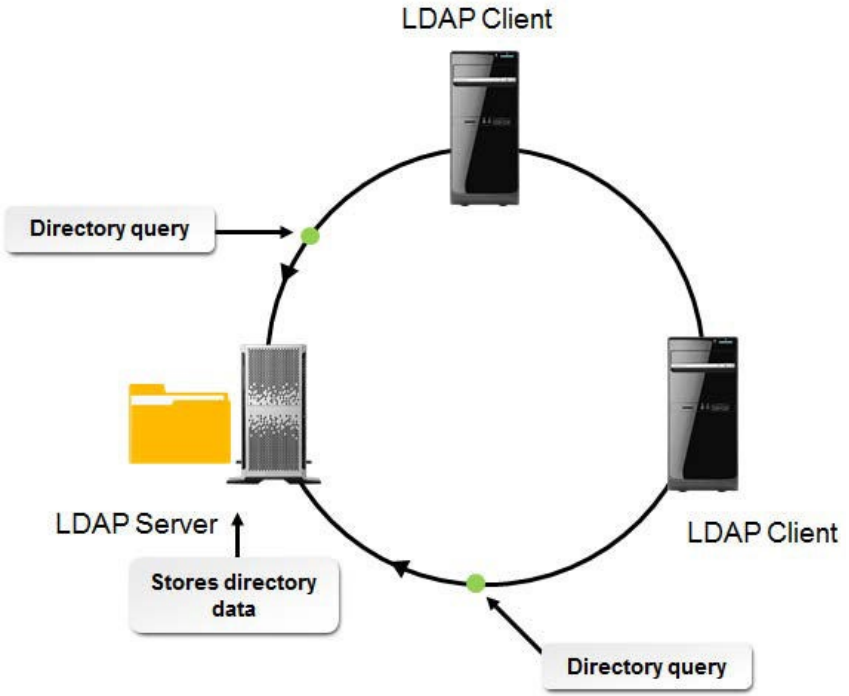
Directory Schema

- The structure of the directory is controlled by a schema that **defines rules** for **how objects are created** and **what their characteristics can be**.
- Most schemas are **extensible**, so they can be modified to support the specific needs of an organization.

Lightweight Directory Access Protocol

- It is a directory access protocol that **runs** over Transmission Control Protocol/Internet Protocol (**TCP/IP**) networks.
- LDAP clients authenticate to the LDAP service, and the **service's schema** defines the tasks that clients can and cannot perform while accessing a directory database, the form the directory query must take, and how the directory server will respond.
- The LDAP schema is **extensible**, which means you can make changes or add on to it.

LDAP clients sending directory queries to an LDAP server.

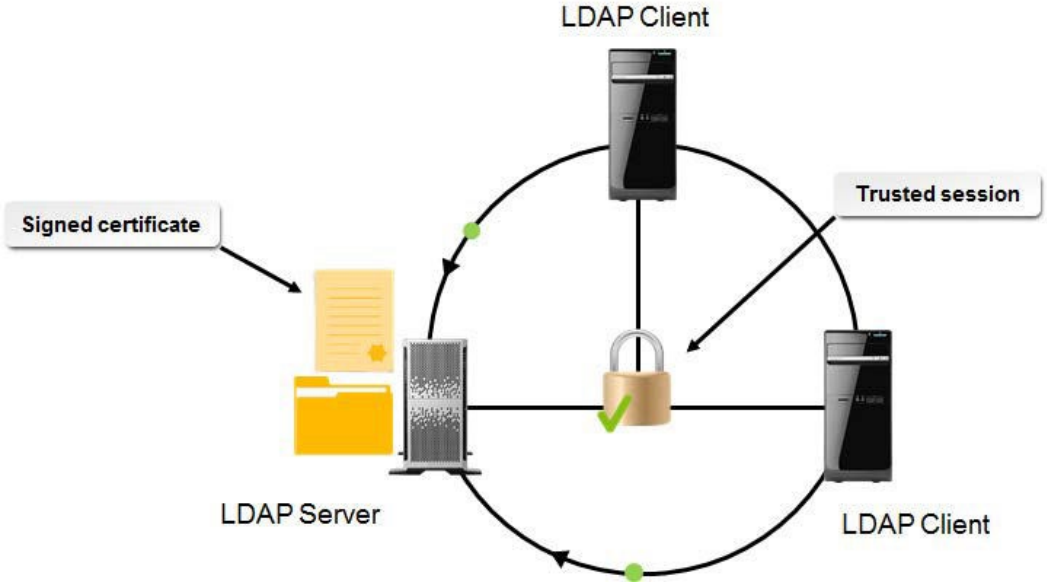


Directory Management Tools

- Most directory services implementations ship with some **management tools** of their own.
- There are a wide variety of **third-party** LDAP browsing and administration tools available from both **open-** and **closed-source** vendors.
- You can create scripts that use LDAP to automate routine directory maintenance tasks, such as
  - Adding large numbers of users or groups
  - Checking for blank passwords or disabled or obsolete user accounts.

Secure LDAP (LDAPS)

- It is a method of implementing LDAP using **Secure Sockets Layer/Transport Layer Security (SSL/TLS)** encryption protocols to prevent **eavesdropping** and **man-in-the-middle** attacks.
- LDAPS forces both **client** and **server** to establish a **secure connection** before any transmissions can occur.
  - If the secure connection is **interrupted** or **dropped**, LDAP likewise closes.
- The server implementing LDAPS requires a **signed certificate** issued by a certificate authority.
  - The client must accept and install the certificate on their machine.



Common Directory Services

- There are a **variety** of robust directory services available, both **paid** and **free**, **open** and **closed** source.
- **Microsoft® Active Directory®**
  - A directory service that **holds information** about all network objects for a single domain or multiple domains.
  - Active Directory **allows administrators** to centrally manage and control access to resources using Access Control Lists (ACLs).
  - It allows users **to find resources** anywhere on the network.
  - Active Directory also **has a schema** that controls how accounts are created and what attributes an administrator may assign to them. Active Directory Application Mode (**ADAM**) is a lightweight version of Active Directory.
- **Sun Java™ System Directory Server**
  - This is the latest version of Sun Microsystems' Directory Server.
  - It was formerly known as Sun ONE Directory Server and iPlanet Directory Server.
  - Sun Java System Directory Server is built with 64-bit technology and marketed toward large installations that require reliable scaling.
  - The software is free, and paid support is available from Sun.

Common Directory Services

- There are a variety of robust directory services available, both paid and free, open and closed source.
- **OpenDS**
  - An open-source directory server that runs on Linux, Unix, Microsoft® Windows®, and Mac OS X®.
  - OpenDS is written by Sun in Java.
  - It supports **LDAPv3** and Directory Service Markup Language version 2 (**DSMLv2**).
- **OpenLDAP**
  - A free, open-source LDAP implementation with distributions available for most operating systems.
- **Open Directory**
  - Apple's customized implementation of OpenLDAP that is part of the Server app for Mac OS X.
  - Open Directory is somewhat **compatible** with both Active Directory and Novell's eDirectory™ and integrates both the LDAP and Kerberos standards.

Directory Service Vulnerabilities

- **There are some common vulnerability areas to be aware of:**
- **All categories of network-based attacks, including:**
  - Denial of Service (DoS)/Distributed Denial of Service (DDoS) attacks.
  - Unencrypted transmission of data.
  - Man-in-the-middle attacks.
  - Packet sniffing/capture attacks.
- **Buffer overflow attacks.**
- **Security of user and administrator accounts and passwords**.

Backing Up Active Directory

- You back up Active Directory by **backing up** the computer's system state data within the Windows Backup utility.
- Backing up the computer's System State Data also backs up the following components:
  - Registry
  - COM+ Class Registration database
  - Boot and system files
  - Certificate Services database (if you have installed Certificate Services on the server)
  - The SYSVOL folder (if the server is a domain controller)
  - The IIS Metabase (if you have installed IIS)

Remote Access Methods

- There are several different methods that organizations can use to provide remote employees and customers with access to their network resources.

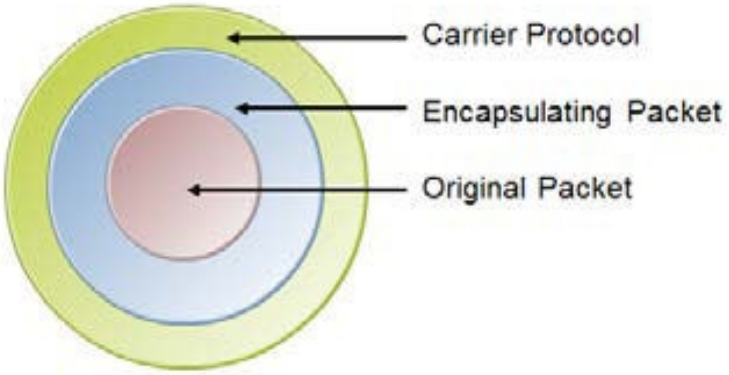
- Companies that require privacy may connect to a gateway remote access server (**RAS**) that provides access control services to all or part of the internal network.

- An intermediate network ➔ such as the Internet ➔ can provide remote access from a remote system or a wireless device to a private network.

- Especially in this case, care must be taken to secure transmissions as they pass over the public

Tunneling

- **Tunneling** is a data-transport technique that can be used to provide remote access in which a data packet is encrypted and encapsulated in another data packet in order to conceal the information of the packet inside.
- This **enables** data from one network **to travel** through another network.
- The tunnel can provide **additional security** by hiding user-encrypted data from the carrier network.
- Tunneling is typically employed as a **security measure** in VPN connections.



Remote Access Protocols

- The **common protocols** used to provide remote access to networks:
  - Point-to-Point Protocol (PPP)
  - Point-to-Point Tunneling Protocol (PPTP)
  - Layer Two Tunneling Protocol (L2TP)
  - Secure Socket Tunneling Protocol (SSTP)

Point-to-Point Protocol (PPP)

- Point-to-Point Protocol (PPP)
  - This is a legacy Internet standard for sending IP datagram packets over serial point-to-point links.
  - Its most common use is for **dial-up** Internet access.
  - It can be used in **synchronous** and **asynchronous** connections.
  - Point-to-Point Protocol over Ethernet (PPPoE) and Point-to-Point Protocol over ATM (PPPoA) are more recent PPP implementations used by many Digital Subscriber Line (DSL) broadband Internet connections.
  - PPP can **dynamically** configure and test remote network connections and is often used by clients to connect to networks and the Internet.
  - It also provides **encryption** for passwords, paving the way for secure authentication of remote users.

Point-to-Point Tunneling Protocol (PPTP)

- Point-to-Point Tunneling Protocol (PPTP)
  - This is a Microsoft VPN Layer 2 protocol that **increases** the security of PPP by providing tunneling and data encryption for PPP packets.
  - It uses the same authentication types as PPP, and is a common VPN method among older Windows clients.
  - PPTP **encapsulates** any type of network protocol and transports it over IP networks.
    - Because it has serious vulnerabilities, PPTP is no longer recommended by Microsoft.

Layer Two Tunneling Protocol (L2TP)

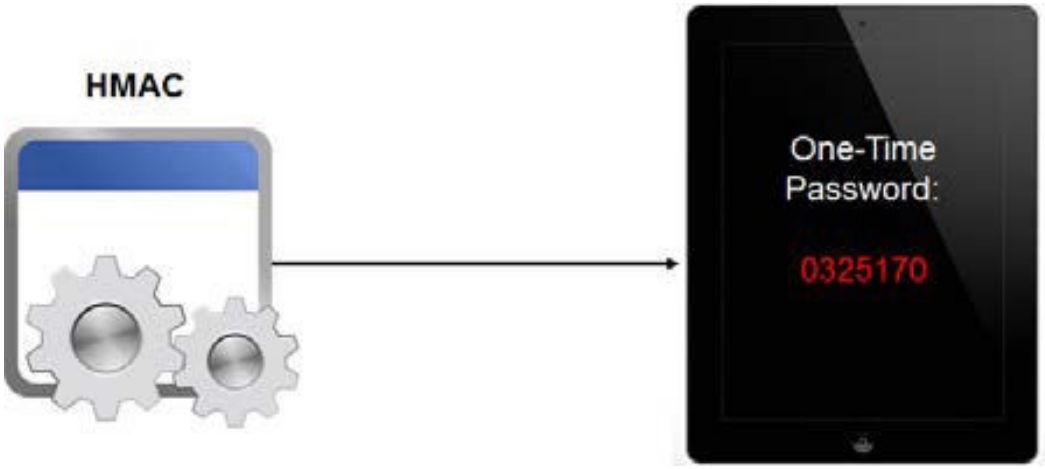
- Layer Two Tunneling Protocol (L2TP)
  - This is an Internet-standard protocol **combination** of PPTP and Layer 2 Forwarding (L2F) that **enables the tunneling** of PPP sessions across a variety of network protocols, such as IP, Frame Relay, or Asynchronous Transfer Mode (ATM).
  - L2TP was specifically designed **to provide** tunneling and security interoperability for client-to-gateway and gateway to-gateway connections.
  - L2TP **does not provide** any encryption on its own and L2TP tunnels appear as IP packets, so L2TP employs IP Security (IPSec) Transport Mode for authentication, integrity, and confidentiality.

Secure Socket Tunneling Protocol (SSTP)

- Secure Socket Tunneling Protocol (SSTP)
  - This protocol **uses** the Hypertext Transfer Protocol over Secure Sockets Layer (HTTP over SSL) protocol and encapsulates an IP packet with a PPP header and then with an SSTP header.
  - The IP packet, PPP header, and SSTP header are **encrypted** by the SSL session.
  - An **IP header** containing the destination addresses is then added to the packet.
  - It is **supported** in all current Windows operating systems.

HMAC-based one-time password (HOTP)

- It is an algorithm that **generates** one-time passwords (OTPs) using a **hash-based authentication code** (HMAC) to ensure the authenticity of a message.
- One-time passwords are meant to **replace insecure static passwords** as an additional factor of authentication.
- The OTP is valid only for that **one** particular session.
- This is a particularly **strong defense** against an attacker who is able to discover someone else's credentials.
- OTPs are also an **alternative** to authentication methods that require installing specific software on each machine that is used to access a system.

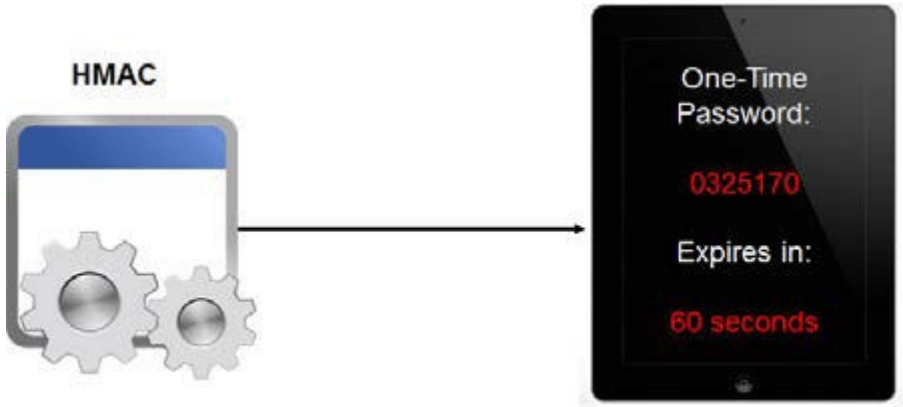


Timed HMAC-based one-time password (TOTP)

- Improves upon the HOTP algorithm by introducing a time-based factor to the one-time password authentication.

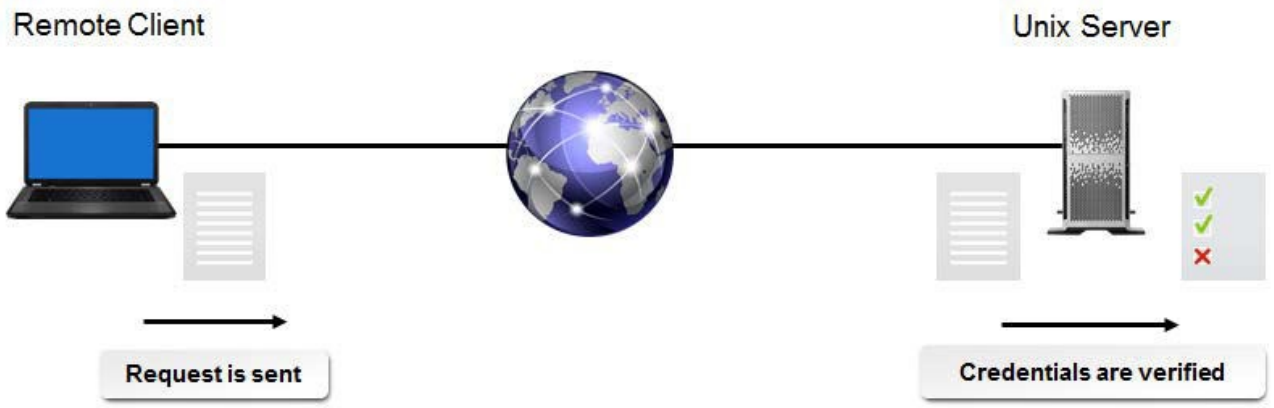
- HOTP and other one-time passwords have a weakness that allows an attacker to take advantage of the password if it is never used.

- The TOTP algorithm **addresses** this security flaw by **generating** and **invalidating** new passwords in specific increments of time, such as 60 seconds.



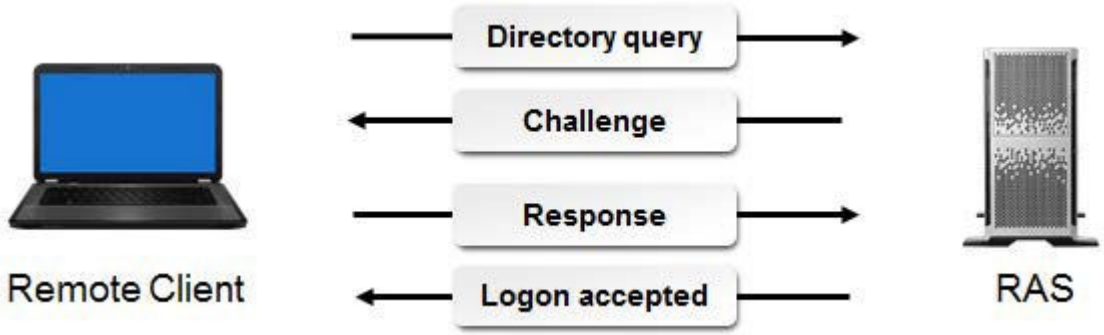
Password Authentication Protocol (PAP)

- It is an authentication protocol that sends **user IDs** and **passwords** as plaintext.
- It is generally used when a remote client is connecting to a non-Windows server that does not support strong password encryption.
- When the server receives a user ID and password pair, it compares them to its local list of credentials.
  - If a match is found, the server accepts the credentials and allows the remote client to access resources.
  - If no match is found, the connection is terminated.
- Because it lacks encryption, PAP is extremely vulnerable and has been largely phased out as a legacy protocol.



Challenge Handshake Authentication Protocol (CHAP)

- It is an **encrypted** authentication protocol that is often used to provide access control for remote access servers.
- CHAP was developed so that passwords would **not have to be sent** in plaintext.
- It is generally used to connect to non-Microsoft servers.
- CHAP uses a combination of Message Digest 5 (MD5) hashing and a challenge-response mechanism, and it accomplishes authentication without ever sending passwords over the network.
- It can **accept connections** from any authentication method **except** for certain unencrypted schemes.
  - CHAP is a more secure protocol than PAP.
  - CHAP is also considered a legacy protocol, particularly because the MD5 hash algorithm is no longer suitably secure.



The CHAP handshake procedure validating user authenticity.

The CHAP Process

The following points describe each step of the CHAP handshake process.

- Step 1 ➔ The remote client requests a connection to the RAS.
- Step 2 ➔ The remote server sends a challenge sequence, which is usually a random value.
- Step 3 ➔ The remote client uses its password as an encryption key to encrypt the challenge sequence and sends the modified sequence to the server.
- Step 4 ➔ The server encrypts the original challenge sequence with the password stored in its local credentials list and compares the results with the modified sequence received from the client:
    - If the two sequences do not match, the server closes the connection.
    - If the two sequences match, the server allows the client to access resources.

Guidelines for Securing Remote Access

- ✓ Set up a VPN for offsite employees to connect to your internal network through the Internet.
- ✓ Use secure tunneling protocols like L2TP with IPSec in your VPN.
- ✓ Avoid insecure tunneling protocols like PPTP.
- ✓ For those employees who access highly sensitive data, implement one-time password authentication.
- ✓ Implement time-based OTPs to mitigate the threat of a session being hijacked.
- ✓ Avoid using PAP and CHAP and other outdated remote access protocols that fail to provide adequate protection.

Pretty Good Privacy (PGP)

- ✓ It is a publicly available email security and authentication utility that uses a variation of public key cryptography to encrypt emails:
  - ✓ The sender encrypts the contents of the email message and then encrypts the key that was used to encrypt the contents.
- ✓ The encrypted key is sent with the email, and the receiver decrypts the key and then uses the key to decrypt the contents.
- ✓ PGP also uses public key cryptography to digitally sign emails to authenticate the sender and the contents.

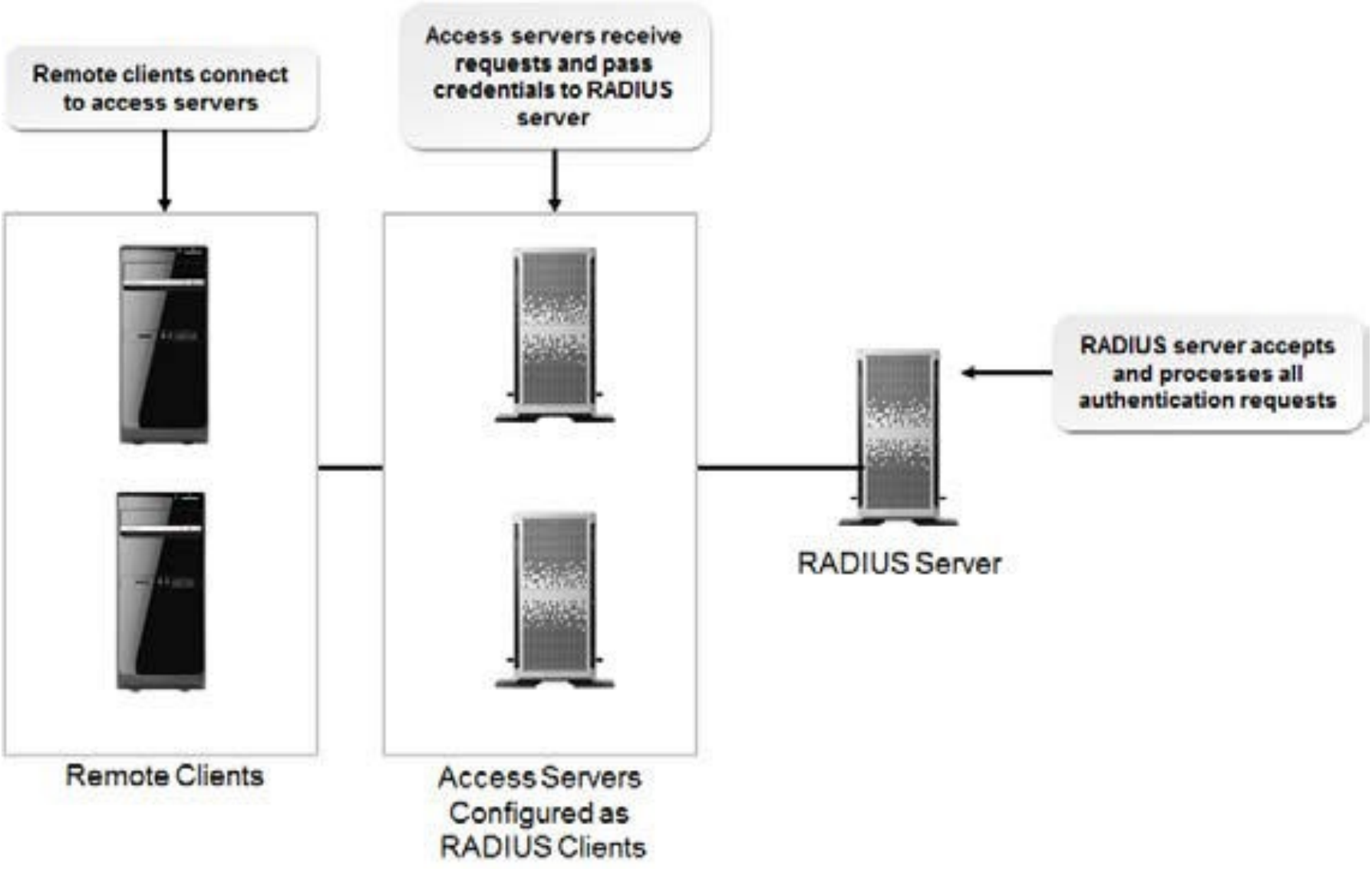
GNU Privacy Guard (GPG)

- ✓ It is a free, open-source version of PGP that provides equivalent encryption and authentication services.
- ✓ GPG is compliant with current PGP services and meets the latest standards issued by the Internet Engineering Task Force (IETF).

Remote Authentication Dial-In User Service (RADIUS)

- ✓ It is an Internet standard protocol that provides centralized remote access authentication, authorization, and auditing services.
- ✓ When a network contains several remote access servers, you can configure one of the servers to be a RADIUS server, and all of the other servers as RADIUS clients.
- ✓ The RADIUS clients will pass all authentication requests to the RADIUS server for verification.
- ✓ User configuration, remote access policies, and usage logging can be centralized on the RADIUS server.
- ✓ In this configuration, the remote access server is generically known as the Network Access Server (NAS).

Remote Authentication Dial-In User Service (RADIUS)



Diameter

- ✓ It is an authentication protocol that improves upon RADIUS by strengthening some of its weaknesses.
- ✓ The name "Diameter" comes from the claim that Diameter is twice as good as RADIUS.
- ✓ Diameter is a stronger protocol in many ways but is not as widespread in its implementation due to the lack of products using it

Network Policy Server (NPS)

- ✓ It is a Microsoft Server 2012 implementation of a RADIUS server.
- ✓ It helps in administrating VPNs and wireless networks.
- ✓ NPS was known as Internet Authentication Service (IAS) in Windows Server 2003.

Terminal Access Controller Access Control System

- The Terminal Access Controller Access Control System (TACACS) and TACACS Plus (TACACS+) protocols provide centralized authentication and authorization services for remote users.

- TACACS+ also supports multi-factor authentication.

- TACACS+ is considered more secure and more scalable than RADIUS because it accepts login requests and authenticates the access credentials of the user.

- TACACS+ includes process-wide encryption for authentication, whereas RADIUS encrypts only passwords.

- The original TACACS and another extension developed by Cisco, XTACACS, have been effectively replaced by the more secure TACACS+.

Kerberos

- ✓ Kerberos is an authentication service that is based on a time-sensitive ticket-granting system.

- ✓ It was developed by the Massachusetts Institute of Technology (MIT) to use a single sign-on (SSO) method where the user enters access credentials that are then passed to the authentication server, which contains an access list and allowed access credentials.

- ✓ Kerberos can be used to manage access control to many different services using one centralized authentication server

The Kerberos Process

- ✓ In the Kerberos process:
- ✓ 1. A user logs on to the domain.
- ✓ 2. The user requests a ticket granting ticket (TGT) from the authenticating server.
- ✓ 3. The authenticating server responds with a time-stamped TGT.
- ✓ 4. The user presents the TGT back to the authenticating server and requests a service ticket to access a specific resource.
- ✓ 5. The authenticating server responds with a service ticket.
- ✓ 6. The user presents the service ticket to the resource.
- ✓ 7. The resource authenticates the user and allows access.

Security Assertion Markup Language (SAML)

- ✓ It is a data format based on XML that is used to exchange authentication information between a service, an identity provider, and the requesting client.
- ✓ SAML coordinates the various identity assertions between these three sources.
- ✓ Using XML as a framework, SAML defines security request information in markup language.
- ✓ This request information contains details such as when a request was issued, what resource is being requested, and any conditions that need to be met.
- ✓ One overarching purpose of SAML is to provide an efficient way of implementing web-based single sign-on authentication across many different protocols.

Identity Management

- ✓ Identity management is an area of information security that is used to identify individuals within a computer system or network.
- ✓ Identities are created with specific characteristics and information specific to each individual or resource in a system.
- ✓ When pertaining to security, restrictions and access controls are assigned using an individual's identity within a system, network, or organization.
- ✓ Security professionals need to apply proper security controls to protect the identities of all individuals within a system and to prevent identity theft by unauthorized users.
- ✓ One aspect of identity management is the protection of personally identifiable information (PII), which is covered later in the course.

Account Management

- ✓ Account management is a common term used to refer to the processes, functions, and policies used to effectively manage user accounts within an organization.

- ✓ Account management job functions should follow the appropriate processes and security guidelines documented in an organizational security policy or account management policy.

- ✓ User accounts allow or deny access to an organization's information systems and resources; therefore, with the proper controls in place, organizations can properly manage accounts.

Account Privileges

- ✓ Account privileges are permissions granted to users that allow them to perform various actions such as creating, deleting, and editing files, and also accessing systems and services on the network.

- ✓ Privileges can be assigned by user or by group.

- ✓ User assigned privileges are unique to each system user and can be configured to meet the needs of a specific job function or task.

- ✓ Group based privileges are assigned to an entire group of users within an organization.
  - ✓ Each user within the group will have the same permissions applied.

Account Policy

- ✓ An account policy is a document that includes an organization's requirements for account creation, account monitoring, and account removal.
- ✓ Policies can include user-specific guidelines or group management guidelines.
- ✓ Some common policy statements include:
  - ✓ Who can approve account creation.
  - ✓ Who is allowed to use a resource.
  - ✓ Whether or not users can share accounts or have multiple accounts.
  - ✓ When and how an account should be disabled or modified after a user access review.
  - ✓ When to enforce general account prohibition.
  - ✓ What rules should be enforced for password history, password strength, and password reuse.

Multiple Accounts

- ✓ Multiple user accounts occur when one individual has several accounts for a system or resource.
- ✓ Accounts may differ depending on the level of access applied, such as a user level account versus an administrator account.
- ✓ It is common within an organization for an individual user to have more than one account for a number of systems.
- ✓ There are issues related to assigning and managing multiple accounts, such as:
  - ✓ Lack of user awareness of the various accounts.
  - ✓ Assigning the right level of data access and permissions to the appropriate accounts.
  - ✓ Managing the privileges, permissions, and data replication for each individual's accounts.

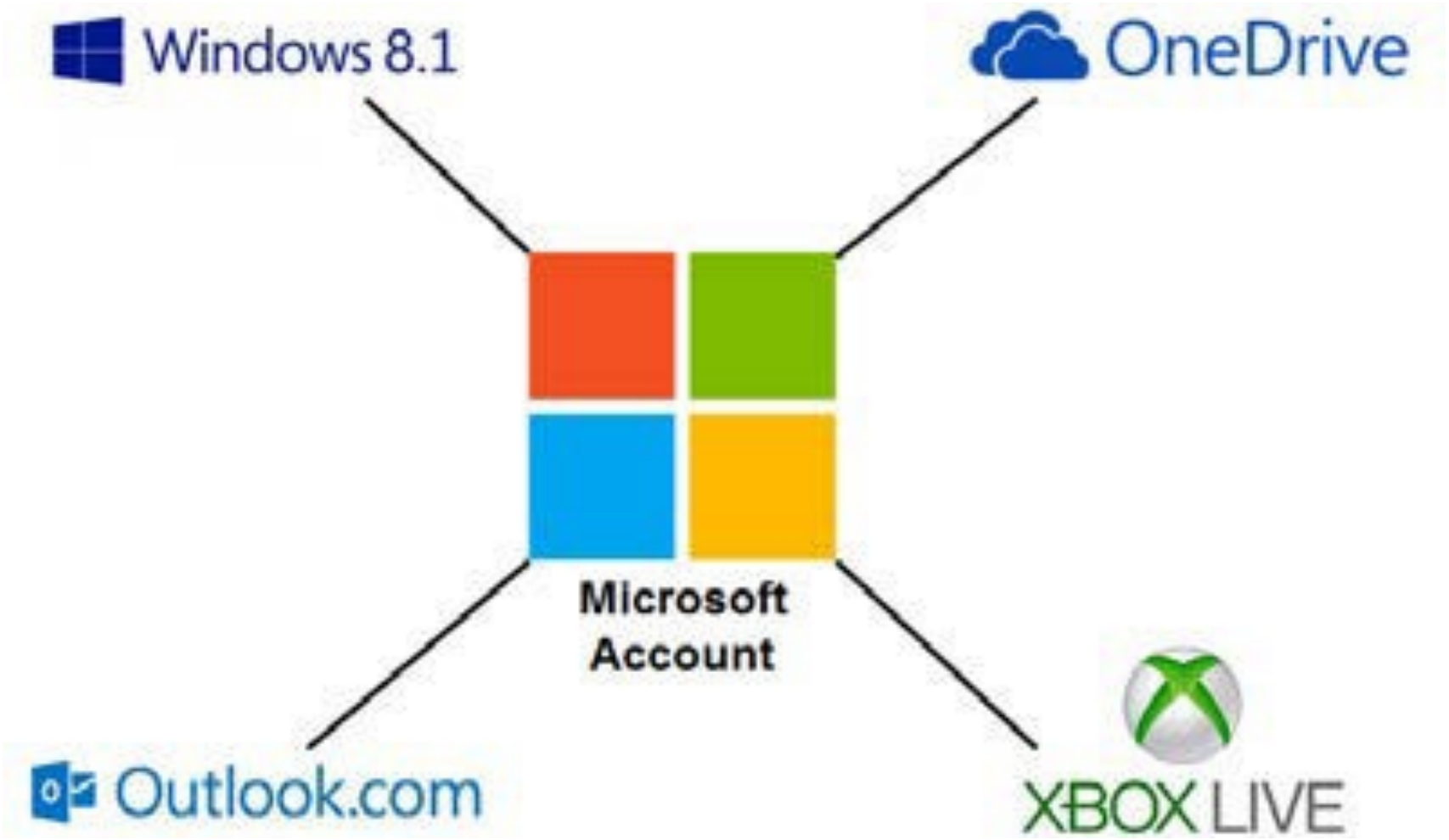
Shared Accounts

- ✓ Shared accounts are accessed by more than one user or resource, and unlike traditional unshared accounts, they are not associated with any one individual.
- ✓ Shared accounts are typically associated with a specific role or purpose that many users can share for a variety of reasons:
  - Anonymous and guest accounts function as a way for visitors to access a system.
  - Temporary accounts are useful for employees or contractors who work for a company inconsistently.
  - Administrative accounts allow multiple authorized professionals access to higher privileges.
  - Batch process accounts allow for easily automating many different types of tasks.

Account Federation

- ✓ Account federation is the practice of linking a single account and its characteristics across many different account management systems.
- ✓ SSO is a subset of account federation that specifically works with authentication, whereas account federation encompasses all of the policies and protocols that contribute to an identity.
  - ✓ This provides a centralized account management structure that eliminates the need for unnecessary account information.
- ✓ Federated accounts not only relieve some of the strain on the host, but users find that streamlining a single account for multiple use cases is much more practical and efficient than needing many different accounts.
- ✓ This also creates a single point of compromise for a user's identity.
  - ✓ If the federated account's credentials are stolen, then an attacker can use that account in all of its different functions.

A Microsoft account can be used across many different systems



Account Management Security Controls

- To maintain and enforce the security needs of an organization, strict account management security controls should be implemented and enforced.

1. User ID and password requirements.
2. Account access restrictions.
3. Account management guidelines.
4. Multiple account guidelines.
5. Continuous monitoring.

Thank you