System Administration & Security

COMP 175 | Fall 2021 | University of the Pacific | Jeff Shafer

Active Directory

Active Directory

Active Directory

Active Directory

- **Organization-wide** centralized management for large computer networks
  - User authentication *(who are they?)*
  - User authorization *(what can they do?)*
  - User auditing *(what did they do?)*
  - Specification and enforcement of security policies
  - Software installation, configuration, updates
  - Individual profiles (consistent across all computers)
- Tracks **objects** in a hierarchical manner
- First released with Windows 2000 Server

Authentication vs Authorization

- Authentication
  - Confirm the user identity
- Authorization
  - Grant access to specific resources

Active Directory Objects

- Security Principle Object
  - Active Directory object that can be authenticated and assigned permissions
  - Example: User account, computer account, security group
- Each security principle has
  - GUID – 128 bit Globally Unique ID
  - SID – Security Identifier

Active Directory Objects: User

- **User** is part of organization
- Unique identity within the domain
  - Authenticated by domain
  - Obtains authorization from domain for resources
- Login
  - Username & Password?
  - Username & Smart Card?

Active Directory Objects: Computer

- **Computer** is part of organization
- Individual computers, workstations, servers, …
- Unique account within the domain
  - Authenticated by domain
  - Obtains authorization from domain for resources

Active Directory Objects: Groups

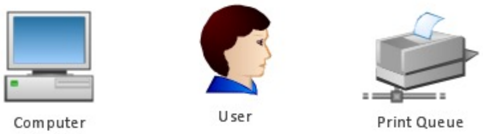
- **Groups**
  - Contains *members* which can be any valid AD object
  - “Domain Admin”
  - “Domain Users”
  - “CTC Printers”
- All permissions, authorizations, and restrictions applied to the group apply to all members of the group

Active Directory Objects: Organizational Unit

- **Organization Unit (OU)**
  - Contains many objects, computers, groups, and *other organization units*
  - Parent / child relationship
    - Any privilege of the parent will be inherited by the child by default
- Intended to mirror organizational structure
  - Faculty / Staff / Students?
  - HR / Finance / Sales / Engineering / Facilities?
  - Seattle office / SF office / NYC office?

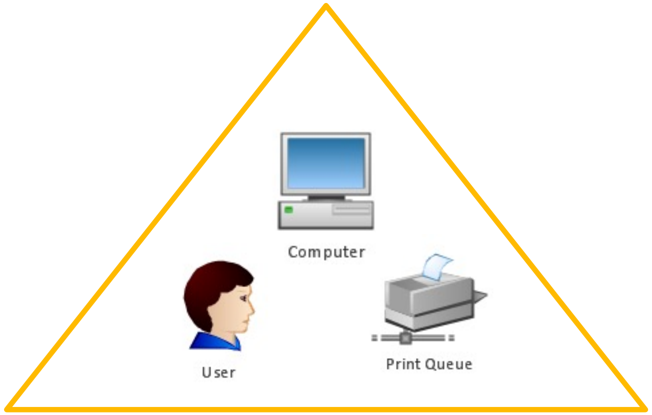
Active Directory Objects: Leaf vs Container

Leaf Objects



Examples: Computer, User, Printer, ….

Container Object



Examples: Group, Organization Unit, ….

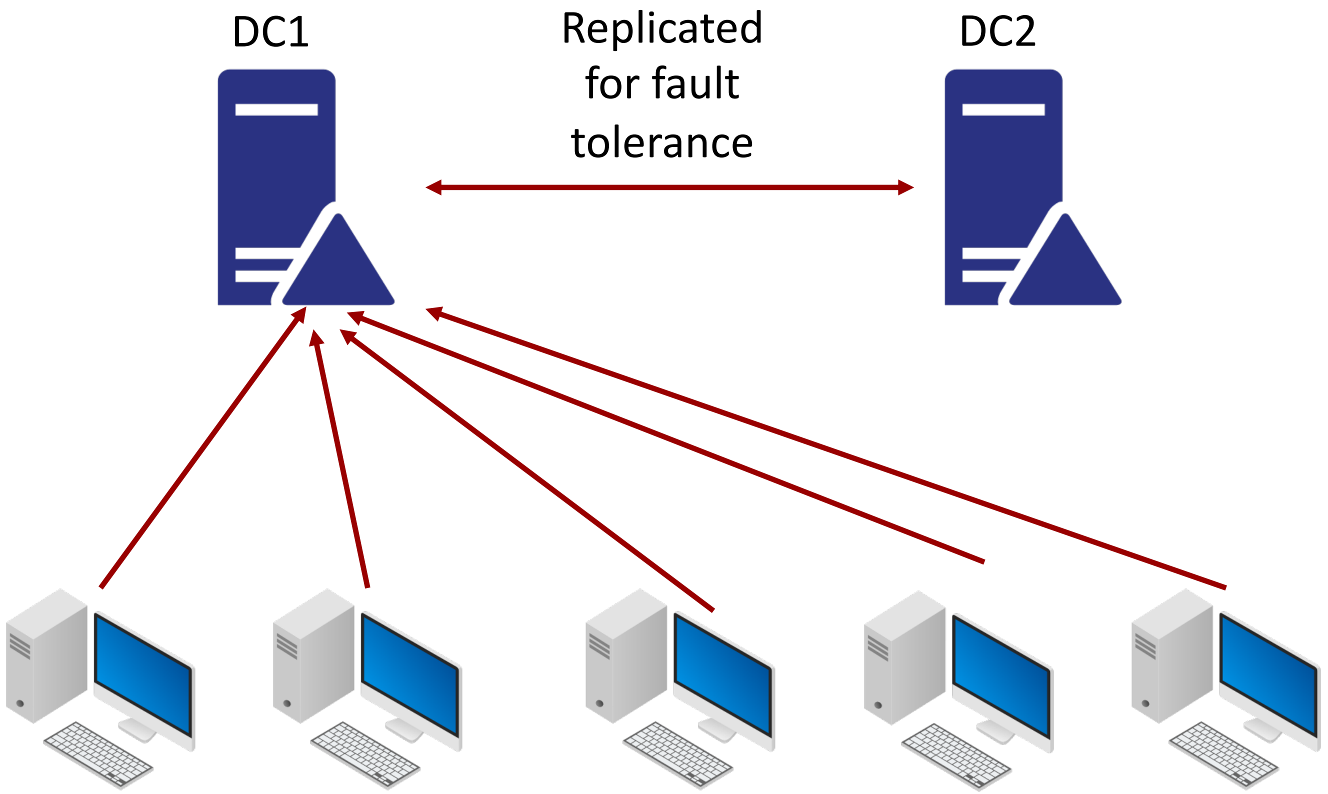
Active Directory Objects: Resources

- Shared Folder
- Printer

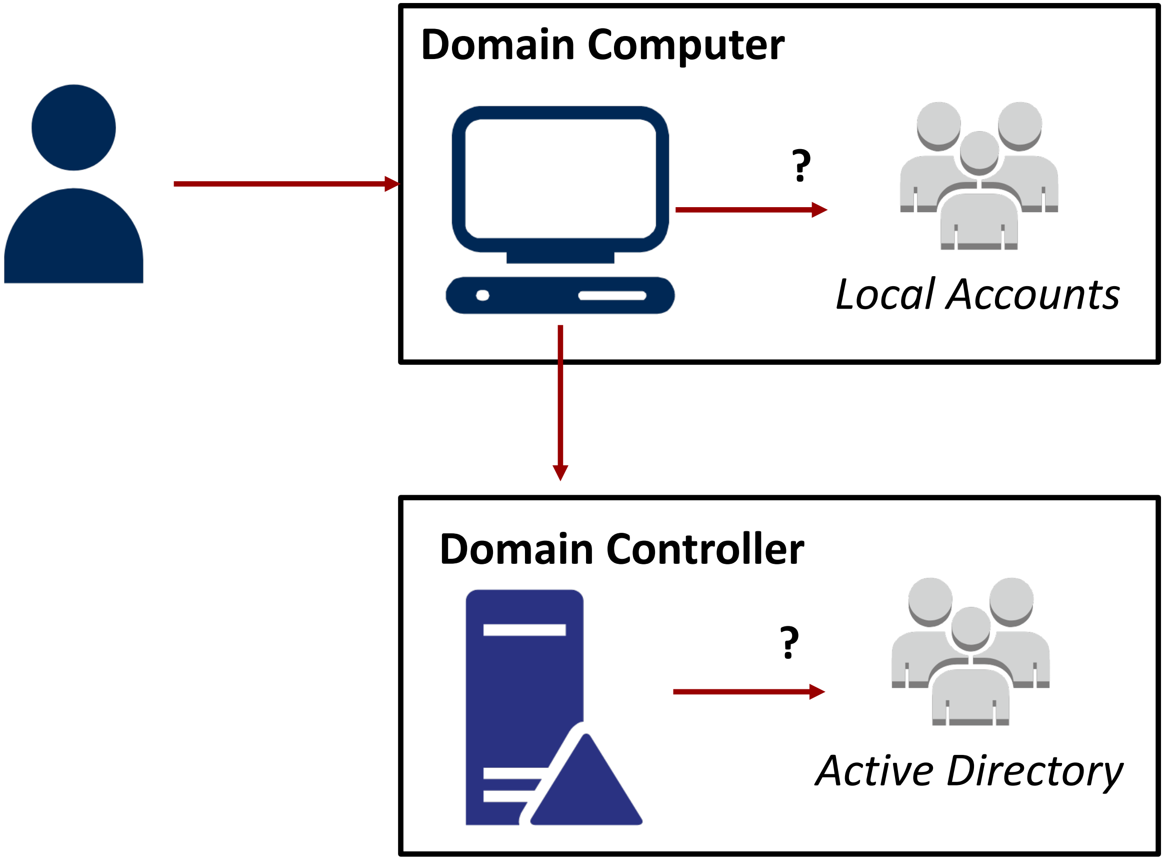
Domain Controller

- **Domain Controller** is a server running the *Active Directory Domain Services* (AD DS) role
- Responds to security authentication requests
- Responsible for
  - Active Directory (AD)
  - Group Policy (GP)

Domain Controller



Login with Domain Controller



(1) Domain computer searches local accounts for matching user

(2) Domain computer sends login request to Domain Controller

Group Policy Management

- Provides remote management for all domain users and computers
- **Group Policy Objects** (GPO) contain client settings
- Group policy can be specified for a user, computer, group, or organization unit
  - Useful for consistent policies across large numbers of users
- Examples
  - Desktop background?
  - Web browser home page?
  - System security settings?
  - Installed applications?

Related Systems

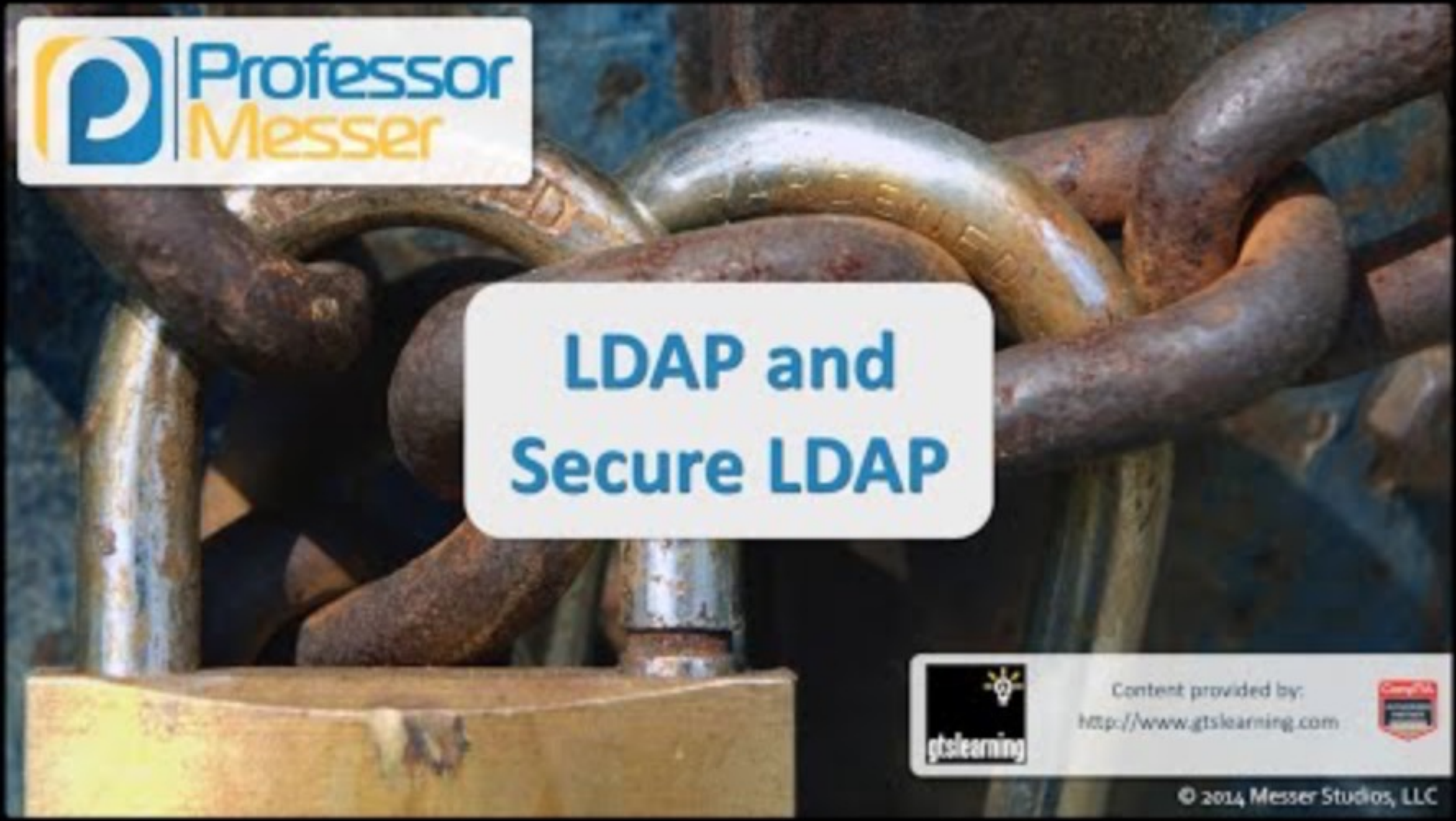
- Active Directory Certificate Services (AD CS)
  - Create and manage public keys for organization
  - Uses: Files, emails, network (VPN, TLS, IPSec)
- Active Directory Federation Services (AD FS)
  - Single Sign-on Service (SSO)
  - Use same credentials for resources within organization and at other organizations (e.g. business partners)

Key Technologies

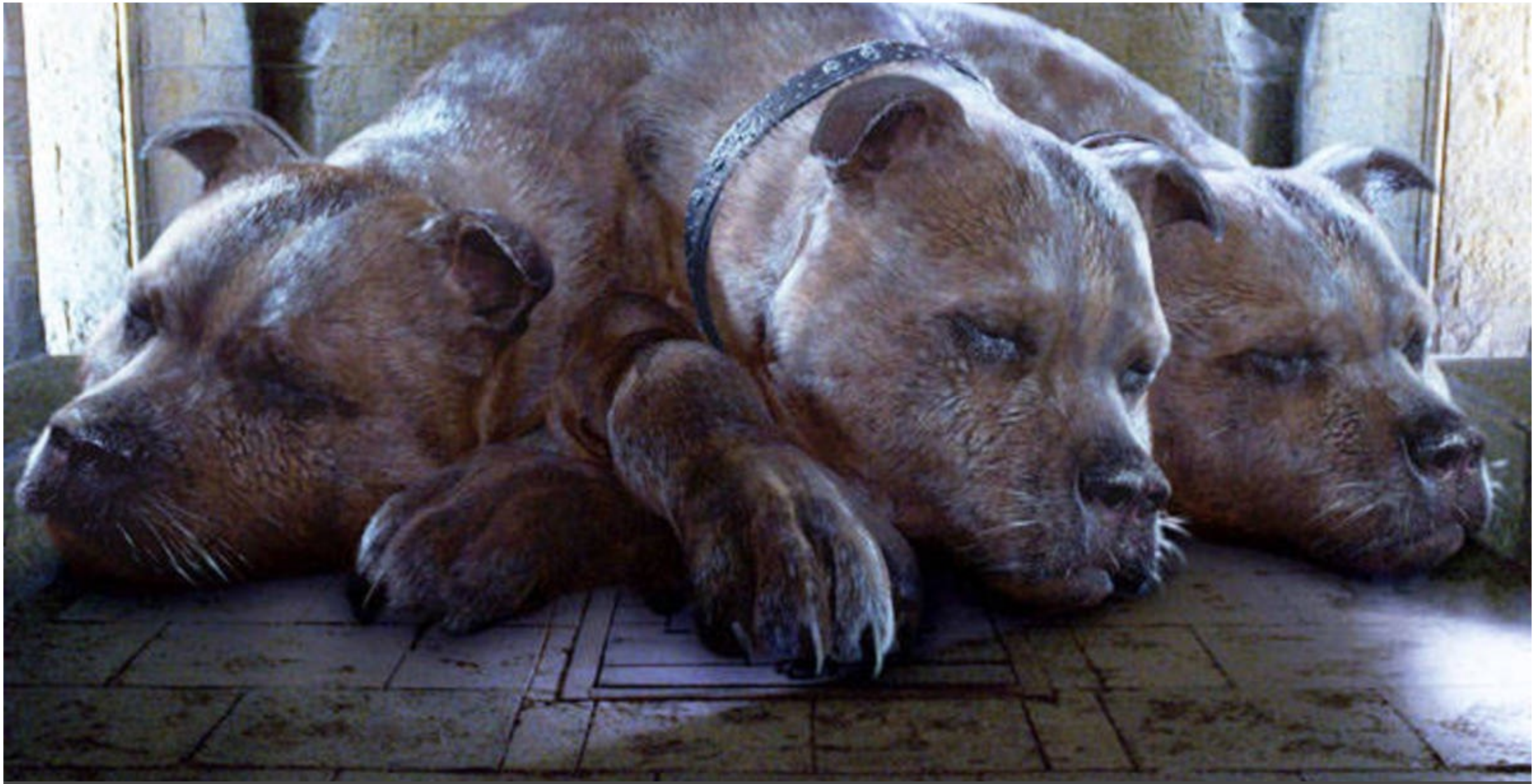
- DNS
  - Resource discovery
- Lightweight Directory Access Protocol (LDAP)
  - Directory (Index)
- Kerberos
  - Authentication

LDAP

LDAP



https://www.youtube.com/watch?v=5rEA7vRV3VE



Kerberos

Cerberus

- Cerberus (Greek: Κέρβερος *Kerberos*) is a multi-headed dog that guards the gates of the Underworld to prevent the dead from leaving
- Kerberos is named after a three-headed dog because authentication is based on interaction between three systems
  - Requesting system (Principal)
  - Endpoint destination system
  - Kerberos server

Kerberos

- Network authentication protocol for client/server applications using symmetric (or public/private key) cryptography
  - Authentication
  - Access control
- **Single Sign-On (SSO)**
- Assumption: Network is insecure – Eve is watching!
- Developed in late 1980’s at MIT as part of *Project Athena*
  - MIT / DEC / IBM project for distributed campus-wide computing environment
- Last updated in 2005 by IETR – Added AES support in v5

Kerberos

- Cross platform
  - Windows, Linux, *BSD, OS X
- Widespread application support*
  - Windows domains
  - SSH (OpenSSH)
  - IMAP, SMTP (Cyrus, sendmail, postfix)
  - CIFS/SMB (Samba, Windows, Netapp)
  - NFS
  - Database (SQL Server, Postgres)
  - HTTP (Apache, nginx, …)
  - DNS (Windows, bind)
  - ** support may be through GSSAPI or SASL layers*

Kerberos & Active Directory

https://www.youtube.com/watch?v=kp5d8Yv3-0c

Kerberos Limitations

- Single point of failure (KDC server)
- Time synchronization required – tickets valid for only 5 minutes
- Compromise of authentication infrastructure allows attacker to impersonate any user (for symmetric cryptography implementation)
- All principals (users, systems) must have a trust relationship with KDC (same realm or trusted realm)
  - Does not work with unknown/untrusted clients

Azure Active Directory

Azure Active Directory

Active Directory Domain Services

- On-Premise / Managed by IT
- Secure object store
  - Users, computers, groups
- Group Policy
  - Management of PCs in domain
- Provides both authentication and authorization

Azure Active Directory

- Cloud-Hosted / Managed by Microsoft
- Secure online authentication store
  - Ties in with application authentication mechanisms (SAML, Oauth) - Single Sign-On
- No concept of “joining servers” or PCs to domain
- No Group Policy
- No OUs or Forests – Flat structure

Active Assignments

- **Project 1**
  - Installation Report – Due Oct 19th
  - Presentation Video – Due Oct 26th
  - Peer Reviews (3) of Video - Due Nov 2nd
- Video
  - 2 minutes – What does app do? Demonstrate that it works
  - 8 minutes – System administration details
    - How to **install** application
    - How to **configure** application
    - How to **secure** application

Active Assignments

- **Lab 9 – Windows Domain Controller** - Due Oct 21st
- **Lab 10 – Windows File Server** - Due Oct 28th
  - Continuation of Domain Controller lab
    - Create a Windows File Server
    - Join it to the domain
    - Demonstrate you have a shared directory
    - Demonstrate that Group Policy can change settings across the domain
    - Demonstrate that the domain controller can remotely access domain computers

Wrap-Up

- Questions?
- Concerns?

- **This Week**
  - Lab 8 – Scripting
  - Lab 9 – Domain Controller and File Server