JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Identity Systems

Security Architecture & Tool Sets

Identity Systems

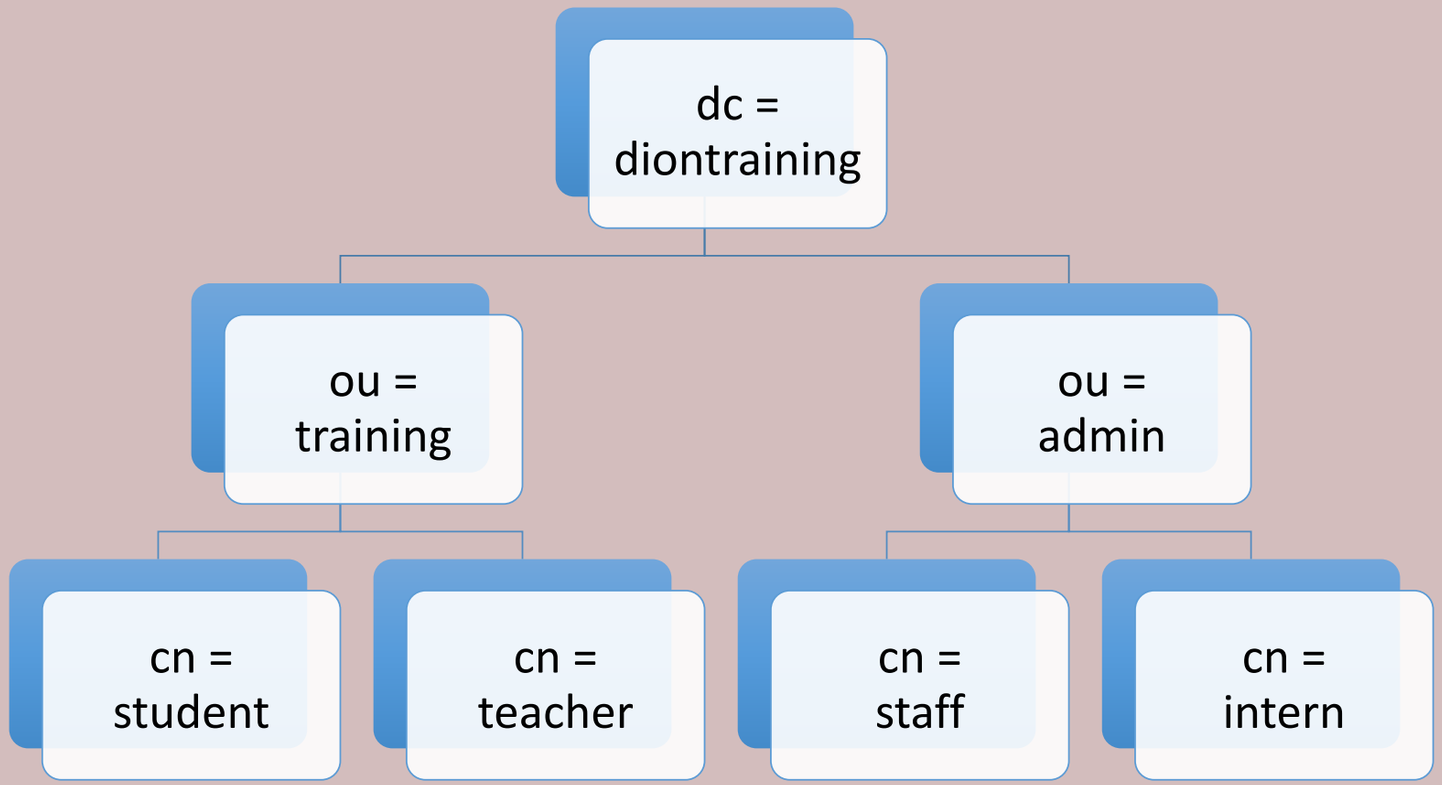
- Provide common functions
  - Identity creation and management
  - Authentication and authorization
  - Federation of identity information

- To provide these functions, we use:
  - Directories
  - Authentication services
  - Identity Management Platforms and federated identity tools

Directory Services

- Used in networks to provide information about systems and users
- LDAP (Lightweight Directory Access Protocol) is commonly used
  - Microsoft's Active Directory, Oracle's Internet Directory, IBM's Security Directory, OpenLDAP, 389 Directory Server, ApacheDS, and OpenDJ
- Can be used to make organizational information available to email and other programs

LDAP Directory Structure



dc = domain name
ou = organizational unit
cn = common name

Securing LDAP

- Enable and require TLS for LDAP query
- Set password storage to use salted hash
- Disable unauthenticated and anonymous LDAP modes (require user/password)
- Replicate LDAP to a redundant server to prevent outages or Denial of Service
- Strong ACLs on LDAP to limit access to objects using least privilege model

LDAP Injection

- Type of attack where improperly filtered input via web applications send arbitrary LDAP queries to the server

- Prevent this by:
  - Escaping all variable using the right LDAP encoding function
  - Use frameworks that automatically protect from injection (*LINQ to Active Directory)*
  - Minimize privileges assigned to LDAP web apps
  - Use input validation to whitelist what is allowed

Authentication Protocols

- Protocols used to supply verification of user's identity to a relying system

- Examples:
  - TACACS+
  - RADIUS
  - Kerberos

TACACS+

- Cisco extension to the Terminal Access Control Access Control System
- Uses TCP to provide AAA services
- Lacks integrity checking of data it sends
  - Subject to replay attacks
- Encryption flaws
  - Encryption key can be discovered by attacker
- Don’t use TACACS+ unless on an isolated network, it is just too flawed…

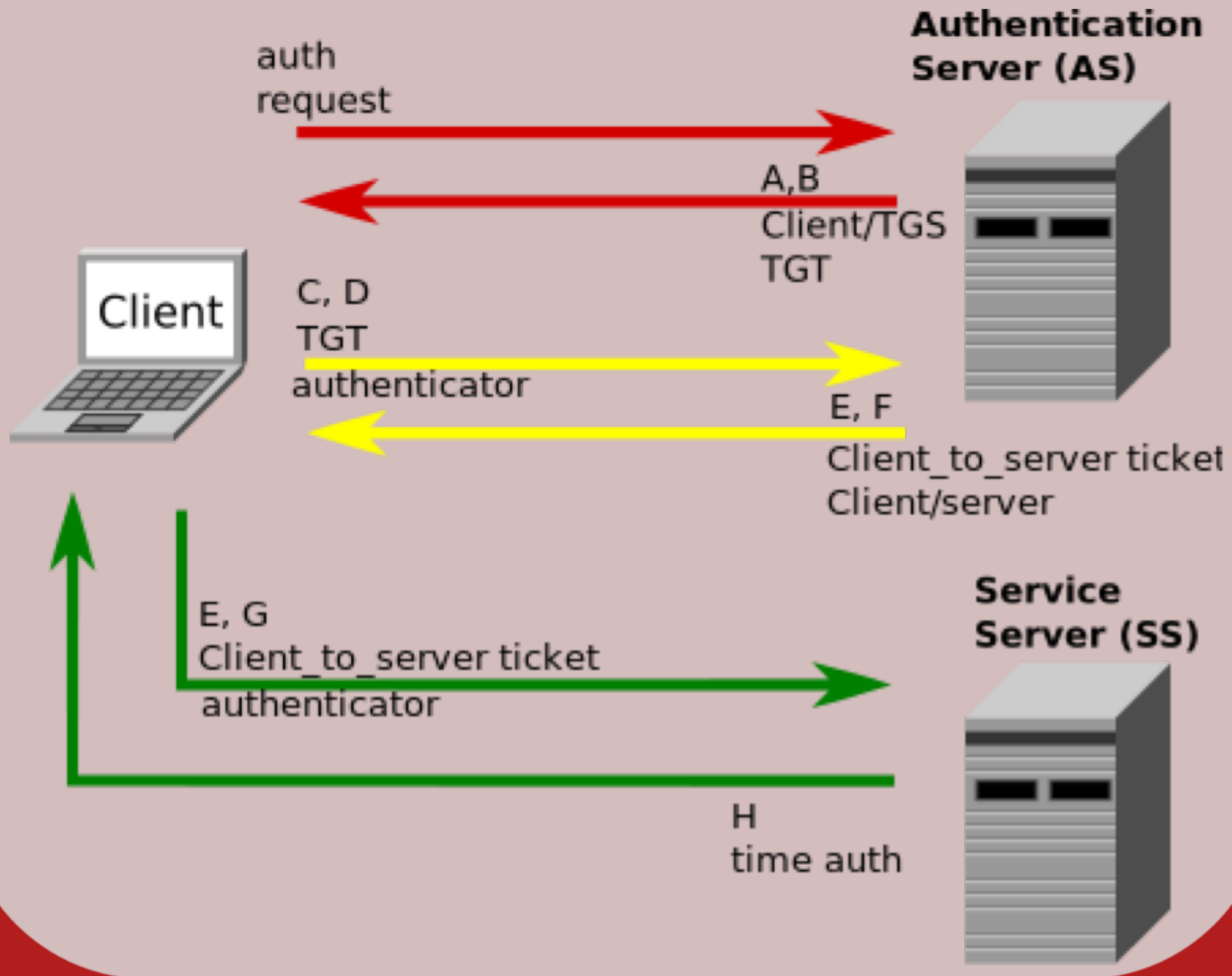
RADIUS

- Remote Authentication Dial-in User Service
- Most common AAA for networks, wireless networks, and other services
- Operates over TCP or UDP in a client-server model
- Password obscured using shared secret and MD5 hash (not considered strong)
- RADIUS traffic should be encrypted using IPSec between endpoints

Kerberos

- Designed with security in mind
- Operates on untrusted networks using encryption of its data
- Principles (users) comprised of three elements:
  - Primary (usually a username)
  - Instance (unique ID incase usernames are similar)
  - Realm (group of primaries)
- Replaced NTLM for AAA in Windows domains

Kerberos Authentication



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Single-Sign-On (SSO)

- Allows users to authenticate once and then be able to use multiple systems

- Examples:
  - LDAP
  - CAS (Central Authentication Service)

- Benefits:
  - Reduce password reuse
  - Fewer password resets and support calls

Shared Authentication

- OpenID
  - Open-source standard for decentralized authentication
  - Uses Google ID to logon to all sites
- OAuth
  - Open authentication standard used to share elements of identify with third-party (ie., Google provides your info)
- OpenID Connect
  - Authentication layer built using OAuth protocol
- Facebook Connect
  - Facebook login to authenticate to other websites and services