CSCD 303

Lecture 5

Fall 2017

Kerberos

Radius, LDAP, Radius used in Authenticating Users

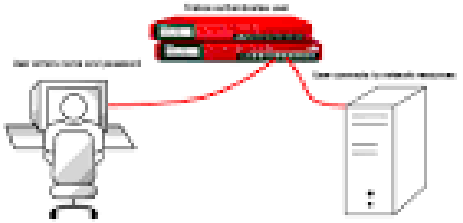
Introduction to Centralized Authentication

- Kerberos is for authentication only and provides Single Sign-on (SSO)
- LDAP can be used for authentication, authorization, and name services (no SSO)
- Active Directory is a directory service with an LDAP interface – based on LDAP
- Use Kerberos for authentication,
- Radius is also used for authentication,
- LDAP for authorization and name services

The Authentication Process in General

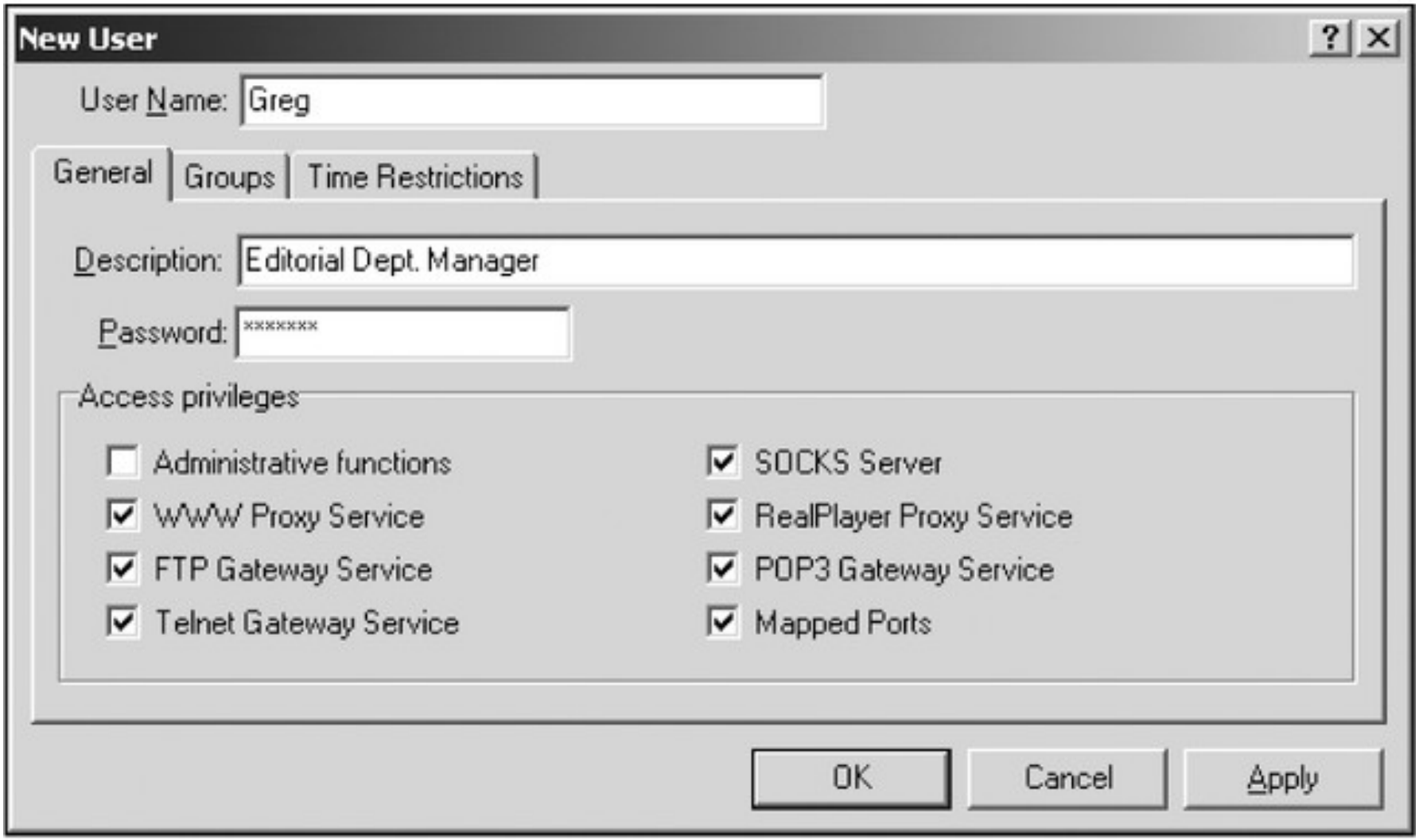
- The act of identifying users and providing network services to them based on their identity
- Two forms
  - Local authentication
  - Centralized authentication service (often uses two-factor authentication)

User Authentication



- Basic authentication; user supplies username and password to access networked resources
- Users who need to legitimately access internal servers in a network must be added to access control lists (ACLs)

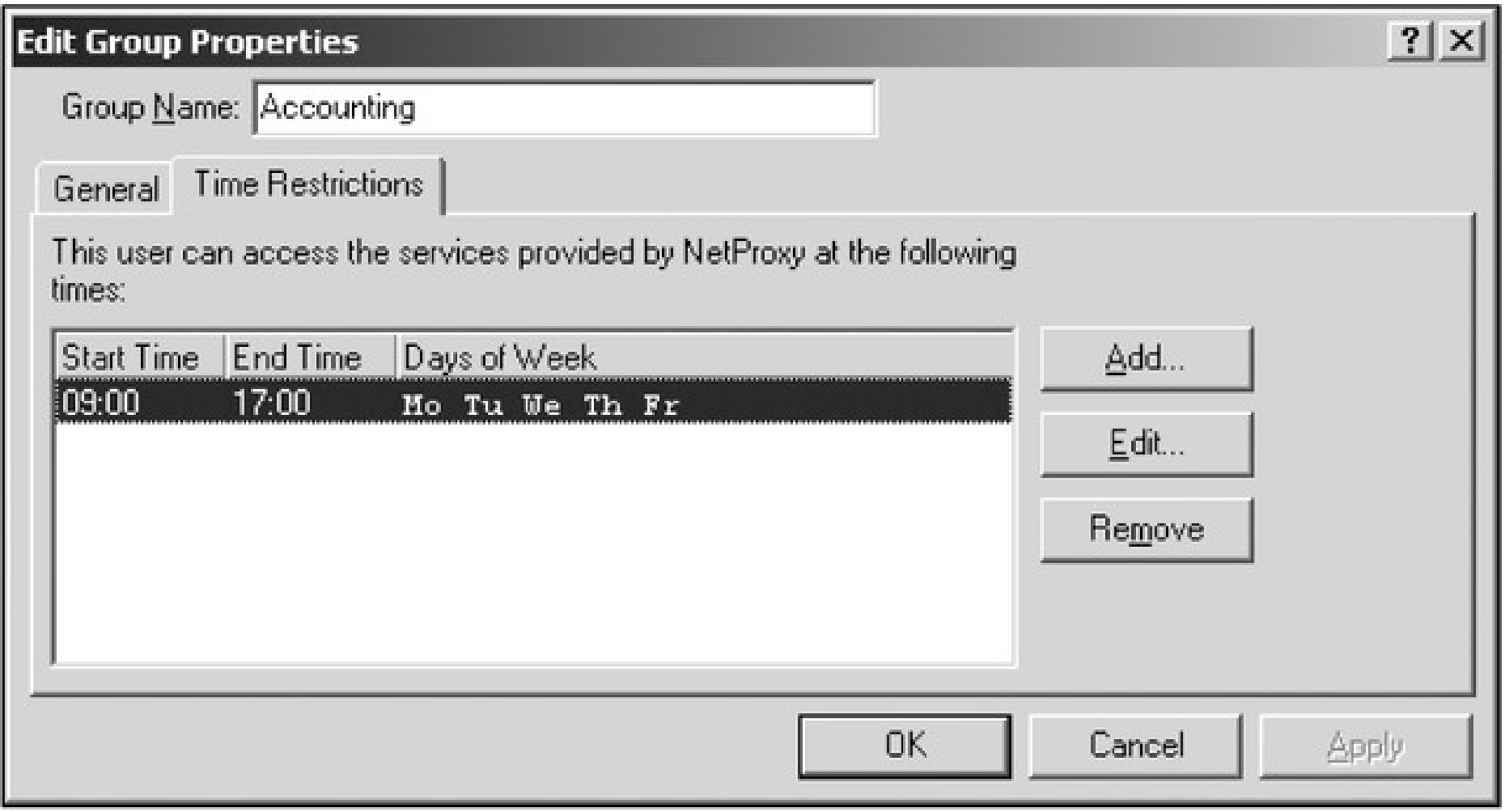
User Authentication Showing Roles



Client Authentication

- Same as user authentication but with additional time limit or usage limit restrictions
  - Notion of paying for services
- When configuring, set up one of two types of authentication systems
  - Standard sign-on system
  - Specific sign-on system

Client Authentication



Session Authentication

- Required any time the client establishes a session with a server of other networked resource

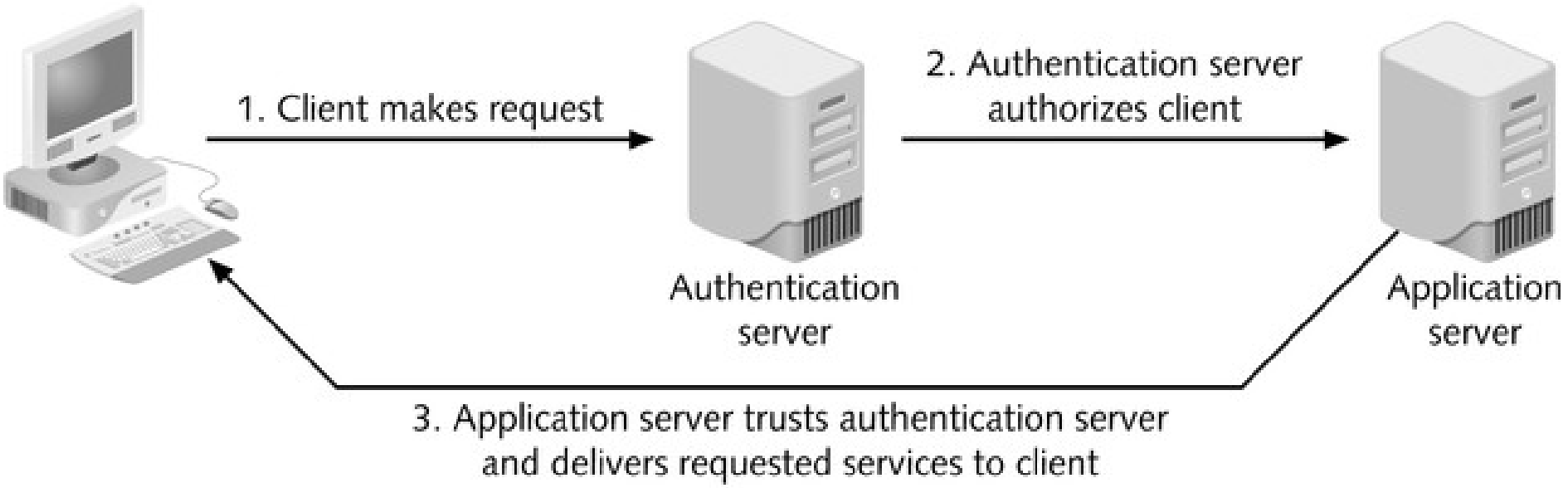
Comparison of Authentication Methods

Method	Use When…
User Authentication	■ You want to scan the content of IP packets. ■ The protocol in use is HTTP, HTTPS, FTP, rlogin, or Telnet. ■ You need to authenticate for each session separately.
Client Authentication	■ The user to be authenticated will use a specific IP address. ■ The protocol in use is not HTTP, HTTPS, FTP, rlogin, or Telnet. ■ You want a user to be authenticated for a specific length of time.
Session Authentication	■ The individual user to be authenticated will come from a specific IP address. ■ The protocol in use is not HTTP, HTTPS, FTP, rlogin, or Telnet. ■ You want a client to be authenticated for each session.

Centralized Authentication

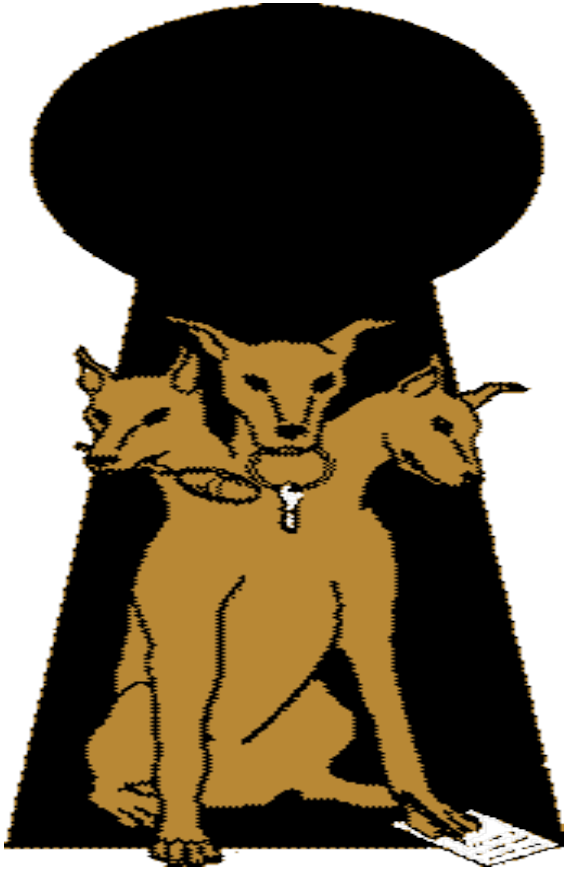
- Centralized server maintains all authorizations for users regardless of where user is located and how user connects to network
- **Most common methods**
  - Kerberos
  - TACACS+ (Terminal Access Controller Access Control System)
  - RADIUS (Remote Authentication Dial-In User Service)
  - Look at each of these ….

Process of Centralized Authentication



Kerberos: etymology

- The 3-headed dog that guards the entrance to Hades
- Originally, the 3 heads represented the 3 A's
  - Authentication
  - Authorization
  - Auditing
- But one A was work enough!



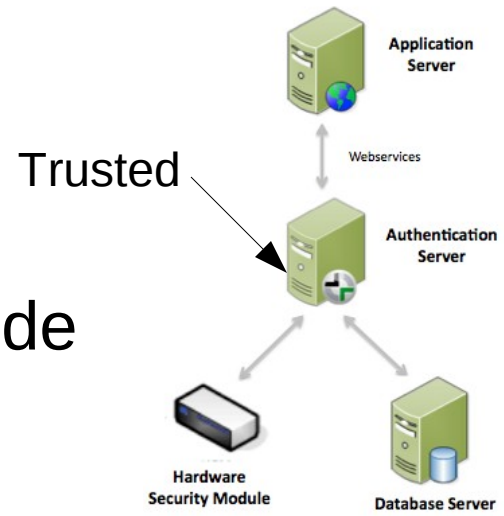
Kerberos

- Provides authentication and encryption through standard clients and servers
- Uses a Key Distribution Center (KDC) to issue tickets to those who want access to resources
- Used internally on Windows 2000/XP and other versions
- Advantages
  - Passwords are not stored on local system
  - Also, widely used in UNIX environment; enables authentication across operating systems

Design Requirements

- Interactions between hosts and clients should be encrypted.
- Must be convenient for users (or they won’t use it).
- Protect against intercepted credentials.

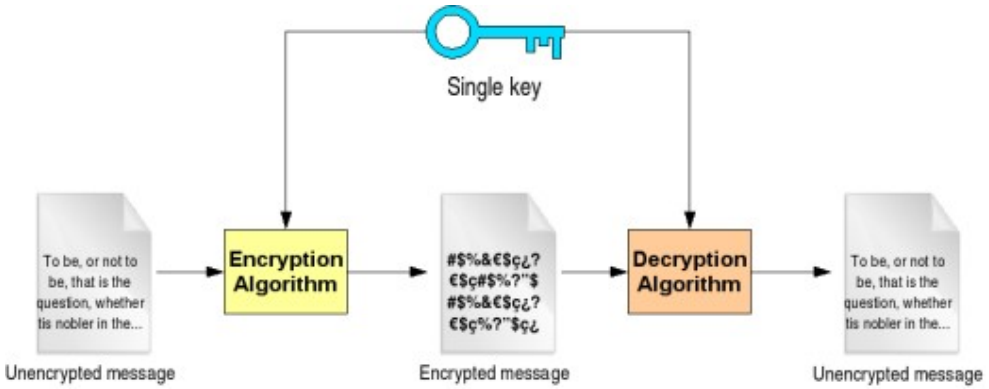
Cryptography Approach



- **Private Key**: Each party uses the same secret key to encode and decode messages
  - Symmetric Cryptography
- Uses a trusted third party which can vouch for the identity of both parties in a transaction.
- Security of third party is critical

Symmetric Key Cryptography

- Aka, Secret Key cryptography
- The same key is used for both encryption and decryption operations (symmetry)
- Examples: DES, 3-DES, AES

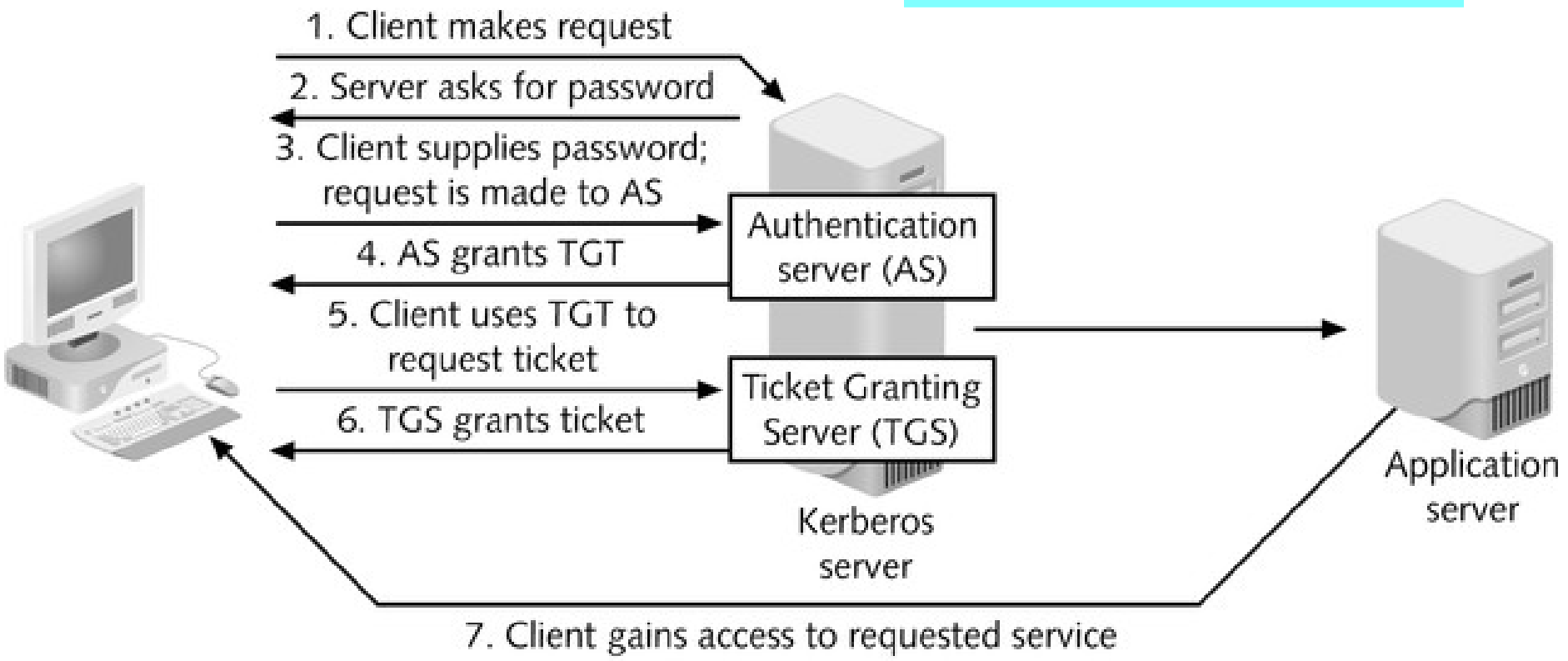


How does Kerberos work?

- Instead of client sending password to application server:
  - Requests **Ticket** from authentication server
  - Ticket and encrypted request sent to application server
- How to request tickets without repeatedly sending credentials?
  - **Ticket granting ticket (TGT)**

Kerberos Authentication

TGT = Ticket Granting Ticket



TACACS+

- Latest and strongest version of a set of authentication protocols for dial-up access (Cisco Systems)
- Provides AAA services
  - Authentication
  - Authorization
  - Auditing
- Uses MD5 algorithm to encrypt data

TACACS+

- Terminal Access Controller Access-Control System (TACACS, usually pronounced like tack-axe)
- Family of related protocols handling remote authentication and related services for networked access control through a centralized server
- Original TACACS protocol, … dates back to 1984,
- Used to communicate with an authentication server,
- Common in older UNIX networks
- Spawned related protocols . one of which is TACACS+

TACACS+

- TACACS allows a client to accept a username and password and send a query to a TACACS authentication server, sometimes called a TACACS daemon or simply TACACSD
- TACACS+ uses TCP
- It determines whether to accept or deny the authentication request and send a response back

RADIUS

- Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized
- Authentication, Authorization, and Accounting (AAA or Triple A) management
- Uses UDP and transmits authentication packets unencrypted across the network
- Provides lower level of security than TACACS+ but more widely supported

Radius

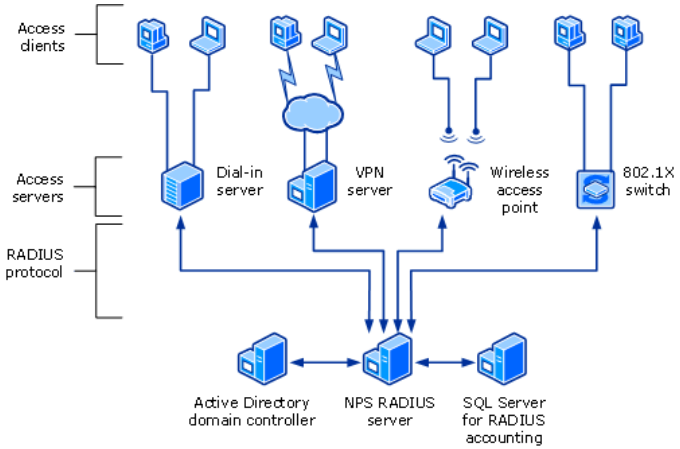
- RADIUS is an AAA protocol which manages network access.
- RADIUS uses two packet types to manage the full AAA process;
- Access-Request, which manages authentication and authorization; and
- Accounting-Request, which manages accounting.

Radius Steps

1. User or machine sends a request to a Network Access Server (NAS) to gain access to a particular network resource using access credentials.
2. In turn,NAS sends a RADIUS Access Request message to RADIUS server, requesting authorization to grant access via RADIUS protocol.
3. RADIUS server checks information is correct using authentication schemes such as PAP, CHAP or EAP

   The user's proof of identification is verified, along with, optionally, other information related to the request,

Radius Steps



5. The RADIUS server then returns one of three responses to the Network Access Server:

1) Access Reject, 2) Access Challenge, or 3) Access Accept.

Access Reject

- The user is unconditionally denied access to all requested network resources.

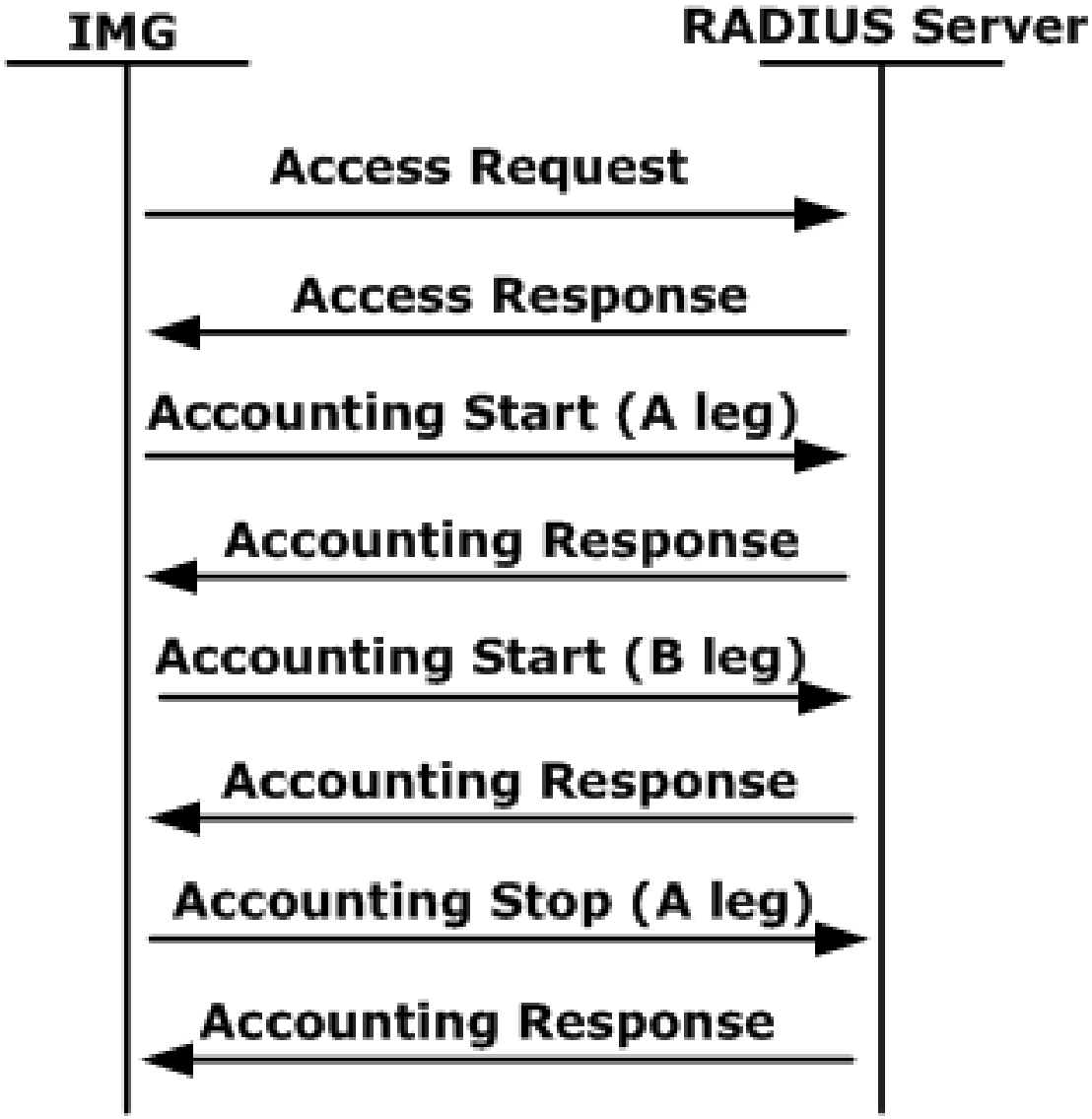
Access Challenge

- Requests additional information from the user such as a secondary password, PIN, token, or card.

Access Accept

- The user is granted access.

Radius Authentication Steps



TACACS+ and RADIUS Compared

- Strength of security
- Filtering characteristics
- Proxy characteristics
- NAT characteristics

Strength of Security

TACACS+	RADIUS
Uses TCP	Uses UDP
Full packet encryption between client and server	Encrypts only passwords –other information is unencrypted
Independent authentication, authorization, and accounting	Combines authentication and authorization
Passwords in the database may be encrypted	Passwords in the database are in clear text

Radius and TACACS+
http://etutorials.org/Networking/Wireless+lan+security/Chapter+2.+Basic+Security+Mechanics+and+Mechanisms/Authentication+and+Identity+Protocols/

LDAP

- Windows Active Directory is based on LDAP
- Active Directory is a directory of objects and provides single location for object management
- Queries to Active Directory uses the LDAP format
- Will cover Active Directory later ...

Single Sign On
(SSO)

Single Sign On

- Traditional Single Sign-On
  - Allows a User to Login Once, Using a Single Authentication Method to Gain Access to Multiple Hosts and / or Applications
  - May Also Provide Access Control / Authorization Features
    - Authorization policies restrict which applications or systems a user has access
    - And what the user can and can't do on these applications and systems

Traditional SSO: Pros and Cons

- **Pros**
  - Very Easy to Use
  - Reduces Support Costs
  - Reduces Logon Cycles
- **Cons**
  - Integration of Legacy Can Be Expensive and Time Consuming
  - Single Point of Attack, attack the SSO host
  - Scripting Solutions Often Lead to Storage of Passwords And IDs on the Client

Traditional SSO: How It Works

- “Authenticate Once To Access Many”
- Login Credentials (ID And Authentication) Usually Stored Locally
- Transparently presented to the System or Application When Needed
  - User does not always know his/her credentials are being presented

Centralized Authentication Summary

- Overview of authentication and its importance to networks and system security
- Authentication server handles
  - Username and password maintenance/generation
  - Login requests
  - Auditing

Examples of centralized authentication systems:

Kerberos

TACACS+

RADIUS

The End

- See Assignments page for new assignment on
    - Authentication

CSCD 303

Lecture 5

Fall 2017

Kerberos

Radius, LDAP, Radius used in Authenticating Users

Introduction to Centralized Authentication

- Kerberos is for authentication only and provides Single Sign-on (SSO)
- LDAP can be used for authentication, authorization, and name services (no SSO)
- Active Directory is a directory service with an LDAP interface – based on LDAP
- Use Kerberos for authentication,
- Radius is also used for authentication,
- LDAP for authorization and name services

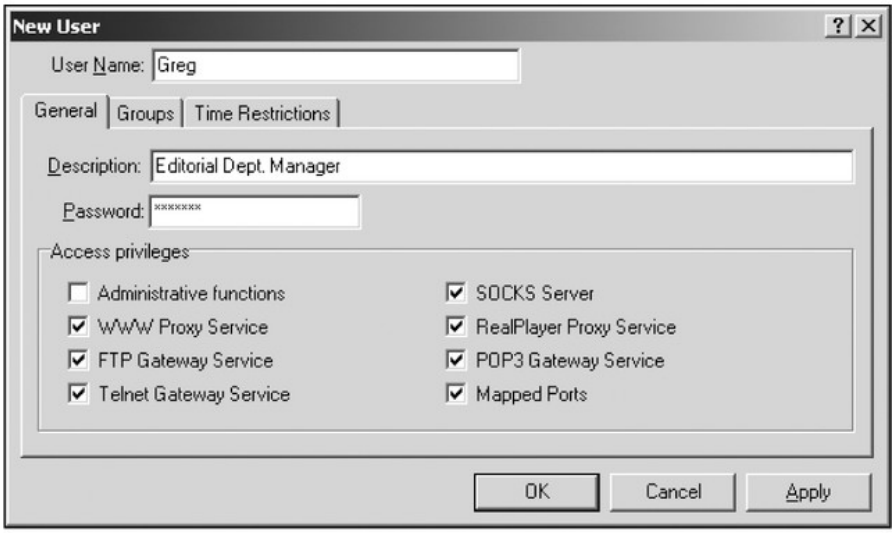
The Authentication Process in General

- The act of identifying users and providing network services to them based on their identity
- Two forms
  - Local authentication
  - Centralized authentication service (often uses two-factor authentication)

User Authentication

- Basic authentication; user supplies username and password to access networked resources
- Users who need to legitimately access internal servers in a network must be added to access control lists (ACLs)

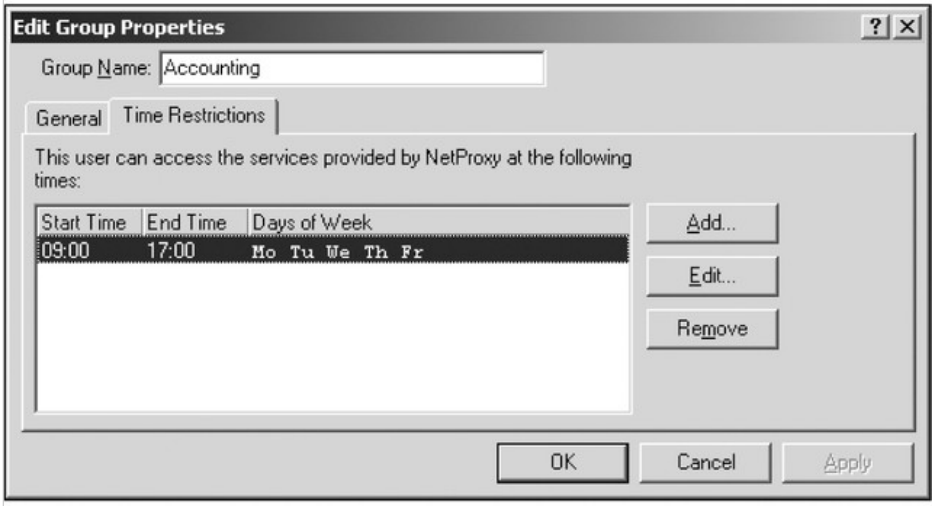
User Authentication Showing Roles



Client Authentication

- Same as user authentication but with additional time limit or usage limit restrictions
  - Notion of paying for services
- When configuring, set up one of two types of authentication systems
  - Standard sign-on system
  - Specific sign-on system

Client Authentication



Session Authentication

- Required any time the client establishes a session with a server of other networked resource

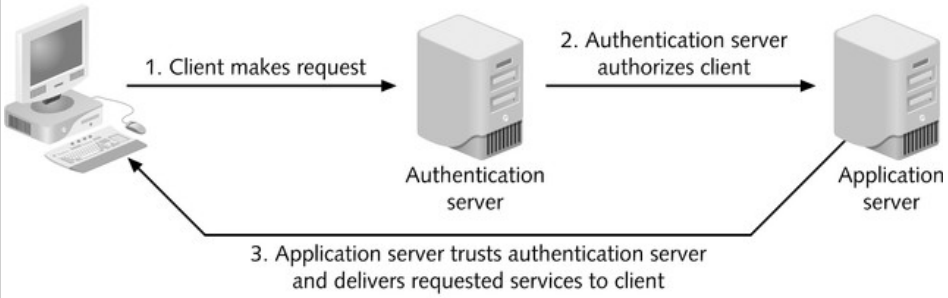
Comparison of Authentication Methods

Method	Use When…
User Authentication	■ You want to scan the content of IP packets. ■ The protocol in use is HTTP, HTTPS, FTP, rlogin, or Telnet. ■ You need to authenticate for each session separately.
Client Authentication	■ The user to be authenticated will use a specific IP address. ■ The protocol in use is not HTTP, HTTPS, FTP, rlogin, or Telnet. ■ You want a user to be authenticated for a specific length of time.
Session Authentication	■ The individual user to be authenticated will come from a specific IP address. ■ The protocol in use is not HTTP, HTTPS, FTP, rlogin, or Telnet. ■ You want a client to be authenticated for each session.

Centralized Authentication

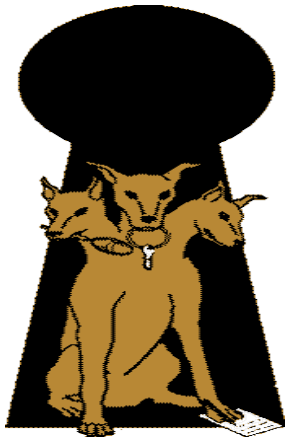
- Centralized server maintains all authorizations for users regardless of where user is located and how user connects to network
- **Most common methods**
  - Kerberos
  - TACACS+ (Terminal Access Controller Access Control System)
  - RADIUS (Remote Authentication Dial-In User Service)
  - Look at each of these ….

Process of Centralized Authentication



Kerberos: etymology

- The 3-headed dog that guards the entrance to Hades
- Originally, the 3 heads represented the 3 A's
  - Authentication
  - Authorization
  - Auditing
- But one A was work enough!



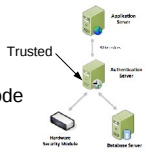
Kerberos

- Provides authentication and encryption through standard clients and servers
- Uses a Key Distribution Center (KDC) to issue tickets to those who want access to resources
- Used internally on Windows 2000/XP and other versions
- Advantages
  - Passwords are not stored on local system
  - Also, widely used in UNIX environment; enables authentication across operating systems

Design Requirements

- Interactions between hosts and clients should be encrypted.
- Must be convenient for users (or they won't use it).
- Protect against intercepted credentials.

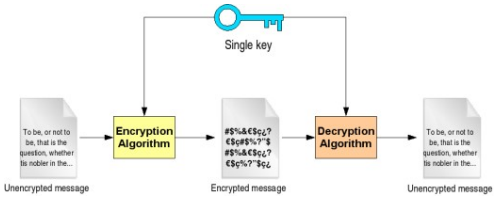
Cryptography Approach



- **Private Key**: Each party uses the same secret key to encode and decode messages
  - Symmetric Cryptography
- Uses a trusted third party which can vouch for the identity of both parties in a transaction.
- Security of third party is critical

Symmetric Key Cryptography

- Aka, Secret Key cryptography
- The same key is used for both encryption and decryption operations (symmetry)
- Examples: DES, 3-DES, AES

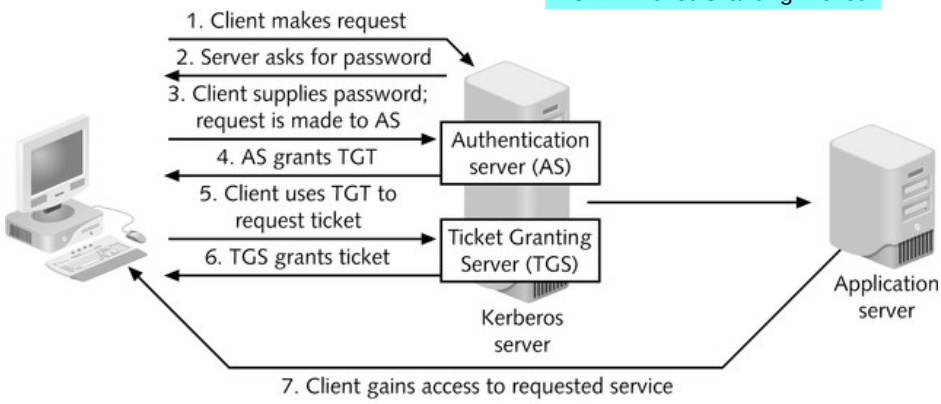


How does Kerberos work?

- Instead of client sending password to application server:
  - Requests **Ticket** from authentication server
  - Ticket and encrypted request sent to application server
- How to request tickets without repeatedly sending credentials?
  - **Ticket granting ticket (TGT)**

Kerberos Authentication

TGT = Ticket Granting Ticket



TACACS+

- Latest and strongest version of a set of authentication protocols for dial-up access (Cisco Systems)
- Provides AAA services
  - Authentication
  - Authorization
  - Auditing
- Uses MD5 algorithm to encrypt data

TACACS+

- Terminal Access Controller Access-Control System (TACACS, usually pronounced like tack-axe)
- Family of related protocols handling remote authentication and related services for networked access control through a centralized server
- Original TACACS protocol, … dates back to 1984,
- Used to communicate with an authentication server,
- Common in older UNIX networks
- Spawned related protocols . one of which is TACACS+

TACACS+

- TACACS allows a client to accept a username and password and send a query to a TACACS authentication server, sometimes called a TACACS daemon or simply TACACSD
- TACACS+ uses TCP
- It determines whether to accept or deny the authentication request and send a response back

RADIUS

- Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized
- Authentication, Authorization, and Accounting (AAA or Triple A) management
- Uses UDP and transmits authentication packets unencrypted across the network
- Provides lower level of security than TACACS+ but more widely supported

Radius

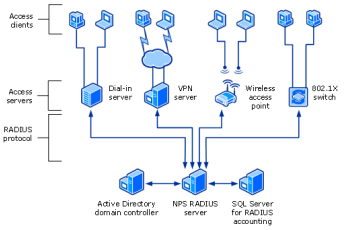
- RADIUS is an AAA protocol which manages network access.
- RADIUS uses two packet types to manage the full AAA process;
- Access-Request, which manages authentication and authorization; and
- Accounting-Request, which manages accounting.

Radius Steps

1. User or machine sends a request to a Network Access Server (NAS) to gain access to a particular network resource using access credentials.
2. In turn,NAS sends a RADIUS Access Request message to RADIUS server, requesting authorization to grant access via RADIUS protocol.
3. RADIUS server checks information is correct using authentication schemes such as PAP, CHAP or EAP

   The user's proof of identification is verified, along with, optionally, other information related to the request,

Radius Steps



5. The RADIUS server then returns one of three responses to the Network Access Server:

1) Access Reject, 2) Access Challenge, or 3) Access Accept.

Access Reject

- The user is unconditionally denied access to all requested network resources.

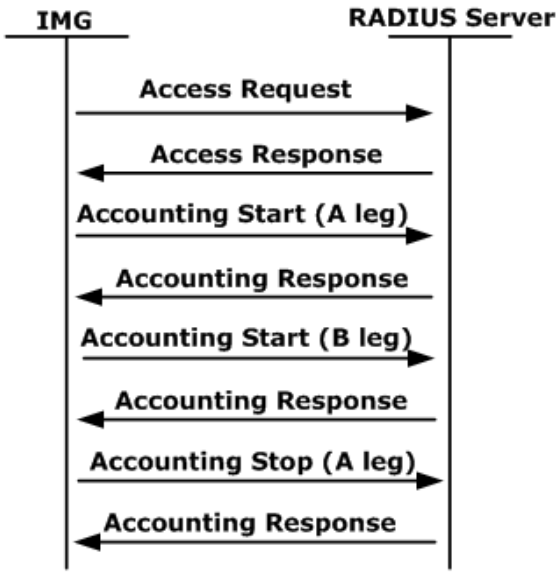
Access Challenge

- Requests additional information from the user such as a secondary password, PIN, token, or card.

Access Accept

- The user is granted access.

Radius Authentication Steps



TACACS+ and RADIUS Compared

- Strength of security
- Filtering characteristics
- Proxy characteristics
- NAT characteristics

Strength of Security

TACACS+	RADIUS
Uses TCP	Uses UDP
Full packet encryption between client and server	Encrypts only passwords –other information is unencrypted
Independent authentication, authorization, and accounting	Combines authentication and authorization
Passwords in the database may be encrypted	Passwords in the database are in clear text

Radius and TACACS+
http://etutorials.org/Networking/Wireless+lan+security/Chapter+2.+Basic+Security+Mechanics+and+Mechanisms/Authentication+and+Identity+Protocols/

LDAP

- Windows Active Directory is based on LDAP
- Active Directory is a directory of objects and provides single location for object management
- Queries to Active Directory uses the LDAP format
- Will cover Active Directory later ...

Single Sign On
(SSO)

Single Sign On

- Traditional Single Sign-On
  - Allows a User to Login Once, Using a Single Authentication Method to Gain Access to Multiple Hosts and / or Applications
  - May Also Provide Access Control / Authorization Features
    - Authorization policies restrict which applications or systems a user has access
    - And what the user can and can't do on these applications and systems

Traditional SSO: Pros and Cons

- **Pros**
  - Very Easy to Use
  - Reduces Support Costs
  - Reduces Logon Cycles
- **Cons**
  - Integration of Legacy Can Be Expensive and Time Consuming
  - Single Point of Attack, attack the SSO host
  - Scripting Solutions Often Lead to Storage of Passwords And IDs on the Client

Traditional SSO: How It Works

- “Authenticate Once To Access Many”
- Login Credentials (ID And Authentication) Usually Stored Locally
- Transparently presented to the System or Application When Needed
  - User does not always know his/her credentials are being presented

Centralized Authentication Summary

- Overview of authentication and its importance to networks and system security
- Authentication server handles
  - Username and password maintenance/generation
  - Login requests
  - Auditing

Examples of centralized authentication systems:

Kerberos
TACACS+
RADIUS

The End

- See Assignments page for new assignment on
    - Authentication