Radius, LDAP, Radius, Kerberos used in Authenticating Users
Authentication and Authorization

- Previously
  - Said that identification, authentication and authorization are critical to computer security, agree?

- **There are two main forms of authentication**
  - Local – user’s machine
  - Remote – User joins a domain, logs in to a web service or other web interface
  
  Sometimes authentication happens behind the scenes by a program or computer acting on your behalf
The Authentication Process in General – Most Cases

• The act of identifying users and providing network services to them based on their identity

• Mainly done through ...
  – Centralized authentication service
Authentication

1. Why do you want or need centralized authentication?

2. What are the advantages of having centralized authentication?
Centralized Authentication

Why do I want Centralized Authentication?

If I manage a domain of multiple machines and devices, want a way to manage users and accounts from one place, convenient and efficient

What are the advantages of having centralized authentication?

Do not configure changes on each separate network device when users are added or deleted, or change passwords

Keep users and their credentials in one place

Easier to manage and maintain consistency
User Authentication

• Basic authentication;
• User supplies username and password to access networked resources
  – For the most part ignoring biometrics
• Users who need to legitimately access internal servers in a network must be added to access control lists (ACLs)
User Authentication
Showing Roles

New User

User Name: Greg

Description: Editorial Dept. Manager

Password: ********

Access privileges

- [ ] Administrative functions
- [x] WWW Proxy Service
- [x] FTP Gateway Service
- [x] Telnet Gateway Service
- [x] SOCKS Server
- [x] RealPlayer Proxy Service
- [x] POP3 Gateway Service
- [x] Mapped Ports

OK | Cancel | Apply
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

Edit Group Properties

Group Name: Accounting

General

This user can access the services provided by NetProxy at the following times:

<table>
<thead>
<tr>
<th>Start Time</th>
<th>End Time</th>
<th>Days of Week</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:00</td>
<td>17:00</td>
<td>Mo Tu We Th Fr</td>
</tr>
</tbody>
</table>

Add... Edit... Remove

OK Cancel Apply
Session Authentication

• Required any time the client establishes a session with a server or other networked resource
• Has an element of time and idea of session expiration
## Comparison of Authentication Methods

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

1. Client makes request
2. Authentication server authorizes client
3. Application server trusts authentication server and delivers requested services to client
Kerberos Authentication Service
Kerberos: etymology

• The 3-headed dog that guards the entrance to Hades
• The 3 heads represent the 3 A’s
  – Authentication
  – Authorization
  – Auditing

Kerberos came from MIT about 1983

Now an open-source standard used in Mac-OS, Windows, some Linux and many Cisco routers
Kerberos

• Provides authentication and encryption through 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 on up

• One major Advantage
  – Passwords are not stored on local system
  – Stored in central database
Design Requirements

• Interactions between hosts and clients should be encrypted ...

• Goals – Wants to overcome
  – Password Sniffing
  – Password database stealing
  – Protect against intercepted credentials, man-in-the-middle attack

• Must be convenient for users (or they won’t use it).
Cryptography Approach

• **Private Key**: Each party uses 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
• DES – Data Encryption Standard
• AES- Advanced Encryption Standard
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)**
    • A special ticket which contains a session key for communication between the client machine and the central KDC server
Kerberos Authentication

1. Client makes request
2. Server asks for password
3. Client supplies password; request is made to AS
4. AS grants TGT
5. Client uses TGT to request ticket
6. TGS grants ticket
7. Client gains access to requested service

TGT = Ticket Granting Ticket
Kerberos Operation

Slides use diagrams from:  https://www.itprc.com/kerberos-authentication-works/

1. Authentication service, or AS, receives the request by the client and verifies that the client is indeed the who he/she claims to be.

2. Upon verification, a timestamp is created. Puts current time in a user session, along with an expiration date.

Default expiration date of a timestamp is 8 hours.

Encryption key is then created. Timestamp ensures that when 8 hours is up, the encryption key is useless.
Kerberos Operation

3. Key is sent back to client in form of a ticket-granting ticket, or TGT. This ticket is issued by authentication service. It is used for authenticating client for future reference.

4. Client submits ticket-granting ticket to the ticket-granting server, or TGS, to get authenticated by TGS.
Kerberos Operation

5. When Client wants to access a service, TGS creates an encrypted key with a timestamp, and grants the client a service ticket.

6. – The client decrypts the ticket and then sends its own encrypted key to the service.
Kerberos Operation

7. Service decrypts the key, and makes sure the timestamp is still valid.
   If it is, the service contacts the key distribution center to receive a session that is returned to the client

8. – The client decrypts the ticket. If the keys are still valid, communication is initiated between client and server
Kerberos Authentication Overview

1. Client authenticates itself to the Authentication Server (AS) which forwards the username to a key distribution center (KDC)

2. KDC issues a ticket-granting ticket (TGT), which is time stamped and encrypts it using the ticket-granting service's (TGS) secret key and returns the encrypted result to the user's workstation

3. Done infrequently, typically at user logon;

4. TGT expires at some point although it may be renewed by the user's session manager while they are logged in
Advantages of Kerberos

- Authentication server keeps a centralized database storing the secret keys of the users and services
- Designed to be secure over insecure networks
- Resistant to attackers and eavesdroppers
- Symmetric key encryption is computationally efficient
- Kerberos centralizes authentication for an entire network—rather than storing sensitive authentication information at each user’s machine
  - Data is only maintained in one presumably secure location
Disadvantages of Kerberos

• What are some disadvantages?
  • Kerberos has a single point of failure: if the Key Distribution Center becomes unavailable, the authentication scheme for an entire network may cease to function
  • If an attacker compromises the KDC, the authentication information of every client and server on the network would be revealed
  • Kerberos requires that all participating parties have synchronized clocks, since time stamps are used.
TACACS and TACACS+

- Terminal Access Controller Access-Control System (TACACS) is a protocol “set”
  - Created and intended for controlling access to UNIX terminals
  - Cisco created a new protocol called TACACS+, which was released as an open standard in the early 1990’s
  - Not backwardly compatible with TACACS
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+

• TACACS lets client to accept username and password
  – Sends query to TACACS authentication server, sometimes called a TACACS daemon or simply TACACSD

• TACACS+ uses Transmission Control Protocol (TCP), reliable network protocol
  – It determines whether to accept or deny authentication request and send a response back
TACACS+

- An example is Cisco switch authenticating and authorizing administrative access to switch’s IOS
- The switch is the TACACS+ client, and Cisco Secure ACS is the server.
TACACS+ Usage Today

- Device administration can be interactive with need to authenticate once, but authorize many times during a single administrative session in command-line of device.
- A router or switch may need to authorize a user’s activity on a per-command basis.
- TACACS+ is designed to accommodate that type of authorization need.
- As name describes, TACACS+ was designed for device administration AAA, to authenticate and authorize users into mainframe and Unix terminals, and other consoles.
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 Components

RADIUS includes three components:
An Authentication server,
Client protocols, and an Accounting server

RADIUS server portion of protocol is usually a background process running on a UNIX or Microsoft Windows server
Radius History and Use

• RADIUS was developed by Livingston Enterprises, Inc. in 1991 as an access server authentication and accounting protocol
  • Later became an Internet Engineering Task Force (IETF) standard

• Often used by Internet service providers (ISPs) and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services

• RADIUS is a client/server protocol that runs in the application layer, and can use either TCP or UDP as transport
Radius

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

4. User's identification is verified.
Radius Steps

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


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 – Using CHAP (Example)

CHAP (Challenge-Handshake Authentication Protocol) is a more secure procedure for connecting to a system than the Password Authentication Procedure (PAP)

Here's how CHAP works:

1. The client uses a hash function to calculate a specific value that is then sent to the server, which matches the incoming value against the server’s calculated value, usually a password

2. If the values match, the client is granted server access. Otherwise, the connection is automatically terminated.

PAP only does this once, CHAP does this repeatedly by sending challenge messages that change and that client must respond to

Making sure client has not been replaced by intruder

Also protects against replay attacks, since challenge value changes
Radius also use for Accounting

- Radius has built-in support for Session Accounting
  - When network access is granted by NAS,
  - **Accounting Start** packet is sent to RADIUS server to signal start of user's access
  - "Start" records typically contain user's identification, network address, point of attachment and a unique session identifier
  - When user's network access is closed, the NAS issues a final **Accounting Stop** record to RADIUS server, with final usage in terms of time, packets transferred, data transferred, reason for disconnect and other information related to the user's network access
  - Purpose of this data is that the user can be billed accordingly and also used for network statistical purposes
TACACS+ and RADIUS Compared

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

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

**Purpose:**
- **Device Administration**
- **Network Access**

**Radius and TACACS+**
LDAP
Lightweight Directory Access Protocol

• 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
Implementation of SSO

• SSO Implemented in Many Ways
  • Kerberos is considered an SSO method
  • Smart card technology is SSO
  • OAuth from Google
  • OpenID
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
References

TACACS+

Radius
https://en.wikipedia.org/wiki/RADIUS

Kerberos
https://worldhack001.blogspot.com/2016/05/what-is-kerberos-and-his-advantages-and.html
https://www.itprc.com/kerberos-authentication-works/
The End

• See Assignments page for new assignment on
  • Authentication