A Basic Introduction to Kerberos

Ken Hornstein
NRL
Kerberos Introduction

• A network protocol developed at MIT as part of Project Athena.

• Is a shared-secret, trusted third party authentication system.

• Uses encryption to provide authentication between peers.

• Designed to be used by third-party programs (like OpenAFS).
Basic Kerberos Concepts

- Designed to provide secure authentication (not authorization) between two entities on a network (called principal identifiers or principals for short).

- Every principal is assigned an encryption key (password for users).

- All encryption keys are registered with the Key Distribution Center (KDC).

- Kerberos services (like AFS, IMAP) are referred to as application servers.

- A zone of Kerberos administrative authority is called a realm.
Kerberos Protocol Diagram

1. Send initial ticket request to KDC (clear)

2. KDC sends ticket for service, encrypted with client’s key.

3. Client sends ticket to server (ticket is encrypted with server’s key)
Kerberos Ticket

• Contains the following information:
  • Client identity (kenh@ATHENA.MIT.EDU)
  • Server identity (afs/sipb.mit.edu@ATHENA.MIT.EDU)
  • Expiration time.
  • Session key (for encryption between the client and server)
  • Various other bits.

• Encrypted with a key the client does not know.
The Ticket-Granting Ticket

- Problem with the basic Kerberos scheme is users have to keep entering their password repeatedly.

- Solution to this problem is to create a new service - the Ticket Granting Service (TGS). This service allows a user to acquire tickets for other services.

- Users acquire a Ticket-Granting Ticket at login time, then talk to the KDC to get additional service tickets.
Kerberos Protocol Exchange with TGT

1. Send initial request for TGT to KDC (clear) krbtgt/REALM@REALM

2. KDC sends ticket for TGS, encrypted with client’s key.

3. Client sends ticket request for service (afs/REALM@REALM), includes TGT service ticket.

4. KDC sends ticket for service (afs/REALM@REALM), encrypted with TGT session key.

5. Client sends ticket to server (ticket is encrypted with server’s key)

Steps 1-2 are done at login time, steps 3-5 done for each new service ticket (user password not required).
Kerberos & AFS

- AFS is a Kerberos application service, with a few slight differences.
- In the Unix implementation, the service ticket is placed in the kernel by klog/aklog.
- One service key is shared across all AFS services in a single realm.
- The “traditional” AFS Kerberos (kaserver) doesn’t use the standard Kerberos transport protocol.