NAME

kerberos - introduction to the Kerberos system

DESCRIPTION

Kerberos is a network authentication system. Its purpose is to securely authenticate users and services in an insecure network environment.

This is done with a Kerberos server acting as a trusted third party, keeping a database with secret keys for all users and services (collectively called *principals*).

Each principal belongs to exactly one *realm*, which is the administrative domain in Kerberos. A realm usually corresponds to an organisation, and the realm should normally be derived from that organisation's domain name. A realm is served by one or more Kerberos servers.

The authentication process involves exchange of 'tickets' and 'authenticators' which together prove the principal's identity.

When you login to the Kerberos system, either through the normal system login or with the kinit(1) program, you acquire a *ticket granting ticket* which allows you to get new tickets for other services, such as **telnet** or **ftp**, without giving your password.

For more information on how Kerberos works, see the tutorial at **https://kerberos.org/software/tutorial.html** or the informal "dialogue" at **https://web.mit.edu/kerberos/dialogue.html**.

For setup instructions see the Heimdal Texinfo manual.

SEE ALSO

ftp(1), kdestroy(1), kinit(1), klist(1), kpasswd(1), telnet(1)

HISTORY

The Kerberos authentication system was developed in the late 1980's as part of the Athena Project at the Massachusetts Institute of Technology. Versions one through three never reached outside MIT, but version 4 was (and still is) quite popular, especially in the academic community, but is also used in commercial products like the AFS filesystem.

The problems with version 4 are that it has many limitations, the code was not too well written (since it had been developed over a long time), and it has a number of known security problems. To resolve many of these issues work on version five started, and resulted in IETF RFC 1510 in 1993. IETF RFC 1510 was obsoleted in 2005 with IETF RFC 4120, also known as Kerberos clarifications. With the

arrival of IETF RFC 4120, the work on adding extensibility and internationalization have started (Kerberos extensions), and a new RFC will hopefully appear soon.

This manual page is part of the **Heimdal** Kerberos 5 distribution, which has been in development at the Royal Institute of Technology in Stockholm, Sweden, since about 1997.