Kerberos: Security Authentication Software

Article Created: 10 July 1992
Article Last Reviewed: 7 August 1992
Article Last Updated:

TOPIC ---

Have you heard of a program called Kerberos? It's somehow being used in conjunction with Informix at one of my accounts.

DISCUSSION ---

We found this information on Kerberos in the Internet RFC (Request for Comment). We should point out that A/UX and Macintosh OS do not support this authentication system.

From Site Security Policy Handbook Working Group RFC 1244

3.9.6 Authentication Systems

Authentication refers to the process of proving a claimed identity to the satisfaction of some permission-granting authority. Authentication systems are hardware, software, or procedural mechanisms that enable a user to obtain access to computing resources. At the simplest level, the system administrator who adds new user accounts to the system is part of the system authentication mechanism. At the other end of the spectrum, fingerprint readers or retinal scanners provide a very high-tech solution to establishing a potential user's identity. Without establishing and proving a user's identity prior to establishing a session, your site's computers are vulnerable to any sort of attack.

Typically, a user authenticates himself or herself to the system by entering a password in response to a prompt. Challenge/Response mechanisms improve upon passwords by prompting the user for some piece of information shared by both the computer and the user (such as mother's maiden name, etc.).

3.9.6.1 Kerberos

Kerberos, named after the dog who in mythology is said to stand

at the gates of Hades, is a collection of software used in a large network to establish a user's claimed identity. Developed at the Massachusetts Institute of Technology (MIT), it uses a combination of encryption and distributed databases so that a user at a campus facility can login and start a session from any computer located on the campus. This has clear advantages in certain environments where there are a large number of potential users who may establish a connection from any one of a large number of workstations. Some vendors are now incorporating Kerberos into their systems.

It should be noted that while Kerberos makes several advances in the area of authentication, some security weaknesses in the protocol still remain.[1]

[1] Bellovin, S., and M. Merritt, "Limitations of the Kerberos Authentication System", Computer Communications Review, October 1990.

Keywords: <None>

==========

19960215 11:05:19.00

Tech Info Library Article Number: 10432