Open Up! Kerberos Server Explained

UFIT

2046 NE Waldo Rd, Suite 2100
Gainesville Florida 32609-8942
(352) 392.2061
<editor@cns.ufl.edu>
Table of Contents

Open Up! Kerberos Server Explained .................................................................3
Open Up! Kerberos Server Explained

On Sunday, November 24, 2002, the UF Kerberos authentication server reached a total of 1,900 days of continuous service. This is more than five years of uninterrupted "up time."

What is Kerberos? The Kerberos protocol was developed at the Massachusetts Institute of Technology (MIT) to enable the transfer of private information over an open network. That is, it is an authentication service that validates the identities of users who request networked application services while protecting the passwords that users offer as proof of identity.

Just about everyone at UF has used -- or will use -- the UF Kerberos service. Each time a GatorLink mailbox is accessed, the mailbox owner is validated via Kerberos. Anyone who has processed grades, travel, or used similar online administrative applications that require a GatorLink password, has used the Kerberos authentication service.

Why do we need a service like this when we have passwords to protect our accounts? Just as we would not wish to hang our house keys on the outside of the front door where anyone could use them, we also do not wish to store them inside our locked homes. We must find a reasonably secure place to store our house keys that still allows accessibility to the house.

Passwords that are submitted over an open network are vulnerable to hackers who "listen in" to the network. We read about this in the news often these days. And, if we rely too heavily on firewalls (another security device) to protect accounts and passwords, we run the risk of restricting legitimate academic access to the Internet just as if we had locked our keys inside our homes. The Kerberos protocol is a middle-ground solution; it is the reasonably safe place.

Kerberos uses symmetric cryptography, that is, it uses the same key to encrypt and decrypt a message. Since it uses the same key for each function, it is important to keep the key secret. This is why it is also called secret-key cryptography.

How is this different from our need to protect user passwords? It isn't. But we can employ the user passwords locally to begin the authentication process without sending them over the open network. Once Kerberos is satisfied that you are the right person, Kerberos will issue a ticket (secret key) that accompanies each message over the network. The ticket labels the user as "trusted" and allows the messages to be encrypted and decrypted as necessary without sending the password with the message.

And a ticket can be reused. This means that if a user logs on to one application that requires GatorLink authentication, she can move to other applications without resubmitting her GatorLink account password until the ticket expires. Tickets do not last forever so there is a lesser risk of exposure than if the actual user password were sent over the network.

Unfortunately, on December 15, 2002, the primary Kerberos server was taken off-line. An electrical switch supporting that server was inadvertently turned off by electricians during scheduled maintenance of other equipment.

However, Kerberos authentication is one of our clustered applications. That is, the primary server is always backed up by auxiliary servers that share the work load whenever necessary, making this a very robust application. In this case, other servers in the cluster picked up the responsibility for providing authentication services without any interruption of this service to our customers.
The Open Systems Group staff members are proud to provide this valuable, strong encryption service, to the UF computing community.

Your Comments are Welcome

We welcome your comments and suggestions on this and all UFIT documentation. Please send your comments to:

UF Information Technology

UFIT

2046 NE Waldo Rd, Suite 2100
Gainesville Florida  32609-8942
(352) 392.2061
<editor@cns.ufl.edu>