This document was originally prepared using the SCRIBE document formatting program. To produce this version the SCRIBE manuscript has been ported to pages.app for the Macintosh. The format thus resembles, but is not quite identical to, the original.

Section E.2.2

Kerberos Applications

by S. P. Miller, B. C. Neuman, J. I. Schiller, and J. H. Saltzer

At the current time, this section is nothing but an extract from an early draft of the Kerberos design proposal. It reflects reality only in a distant way.

Targeted Applications

A long term goal is to have a library that can be used to open session and transport layer connections such that one or both parties are authenticated. A secure UDP, TCP, RPC, or RVD interface would allow any service to use Kerberos for authentication with a minimum of effort.

To simplify the initial implementation, though, the user service exchange will take place at the application layer through modifications to the protocols used for TFTP, LPR/LPD, RPC, RVD control, and RLOGIN. Modifications will also be made at the transport layer for the RVD access protocol. *A protocol for access to the news database of the Community Information System project will be developed so that it can easily make use of Kerberos for authentication.*

1. TFTP

The Trivial File Transfer Protocol benefits from the addition of a new message type to initiate an authenticated *connection*. The new message type is identical to a normal connect messsage, but contains an authenticator in addition to the information required for a normal connect. If the user mentioned in the authenticator is a user of the server system then the file transfer proceeds under that user's system id. If not, the file transfer proceeds as if the user were unauthenticated.

2. LPR/LPD

(Plan only—details not yet worked out.) The LPR protocol can be augmented by including an authenticator in data sent at the beginning of each connection. The current line printer daemon accepts print requests only from clients appearing in a list of a trusted hosts. The authenticator will allow the daemon to verify the user's identity directly and compare it with an access control list of allowed users of this line printer.

3. RVD Accesses

The modification to authenticate RVD access involves adding authentication to the initial setup mechanism for a connection. A new packet type, "authenticated spinup" is added to the protocol; it is identical to the normal spinup packet type with the exception that it includes a Kerberos authenticator. For authorization, the RVD server compares the principal identifier in the authenticator with the record of the owner of the pack, and with names found in optional access control list files named in the pack records.

4. RVD Control

The only modification to the RVD control protocol is the addition of an authenticator operand for those operations that previously required a password authenticator The RVD server then decides if the person is authorized to make the requested change on the basis of access control list files at the server.

5. Rlogin

Rlogin is modified so that it will accept an authenticator as proof of identity. Thus, if you can present an authenticator, and you are authorized to use the system, you will be able to *log in* without a password even if you aren't coming from a trusted host. With the addition of Kerberos authentication, it is possible to eliminate completely all reliance on trusted hosts and on .rhosts files.

6. Community Information System

The community information system will be providing a service to the MIT community whereby they may access certain pieces of information from databases including articles in the New York Times, etc. They will maintain their own database of authorized users, but for users in the Athena environment, they would like to use Kerberos for authentication.