Authentication Service

STATUS OF THIS MEMO

    This RFC suggests a proposed protocol for the ARPA-Internet
    community, and requests discussion and suggestions for improvements.
    Distribution of this memo is unlimited.

INTRODUCTION

    The Authentication Server provides a means to determine the identity
    of a user of a particular TCP connection. Given a TCP port number
    pair, it returns a character string which identifies the owner of
    that connection on the server's system. Suggested uses include
    automatic identification and verification of a user during an FTP
    session, additional verification of a TAC dial up user, and access
    verification for a generalized network file server.

OVERVIEW

    This is a connection based application on TCP. A server listens for
    TCP connections on TCP port 113 (decimal). Once a connection is
    established, the server reads one line of data which specifies the
    connection of interest. If it exists, the system dependent user
    identifier of the connection of interest is sent out the connection.
    The service closes the connection after sending the user identifier.

RESTRICTIONS

    Queries are permitted only for fully specified connections. The
    local/foreign host pair used to fully specify the connection are
    taken from the query connection. This means a user on Host A may
    only query the server on Host B about connections between A and B.

QUERY/RESPONSE FORMAT

    The server accepts simple text query requests of the form

        <local-port>, <foreign-port>

    where <local-port>, is the TCP port (decimal) on the target (server)
    system, and <foreign-port> is the TCP port (decimal) on the source
    (user) system.

        For example:

        23, 6191

    The response is of the form

        <local-port>, <foreign-port> : <response-type> : <additional-info>

    where <local-port>, <foreign-port> are the same pair as the query,
    <response-type> is a keyword identifying the type of response, and
    <additional info> is context dependent.

        For example:

        23, 6191 : USERID : StJohns

RESPONSE TYPES

    A response can be one of two types:

    USERID

        In this case, <additional-info> is the printable representation of
        the user identifier of the owner of the connection. The format of
        the returned user identifier is completely system dependent.

    ERROR

        For some reason the owner of the TCP port could not be determined,
        <additional-info> tells why. The following are suggested values
        of <additional-info> and their meanings.

            INVALID PORT

                Either the local or foreign port was improperly specified.

            NO USER

                The connection specified by the port pair is not currently
                in use.

            UNKNOWN ERROR

                Can't determine connection owner; reason unknown.
                Other values may be specified as necessary.

CAVEATS

   Unfortunately, the trustworthiness of the various host systems that
   might implement an authentication server will vary quite a bit. It
   is up to the various applications that will use the server to
   determine the amount of trust they will place in the returned
   information. It may be appropriate in some cases restrict the use of
   the server to within a locally controlled subnet.

APPLICATIONS

   1) Automatic user authentication for FTP.

   2) Verification for privileged network operations. For example,
   having the server start or stop special purpose servers.

DISCLAIMER

   I designed this protocol to allow me to eliminate the bother of
   having to identify myself before continuing an FTP session.

   Since I started work on it, other applications appeared. I have
   tried to consider all of our applications while still making this as
   general as possible.