                    TACACS User Identification Telnet Option

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 following is the description of a TELNET option designed to
    facilitate double login avoidance. It is intended primarily for TAC
    connections to target hosts on behalf of TAC users, but it can be
    used between any two consenting hosts. For example, all hosts at one
    site (e.g., BBN) can use this option to avoid double login when
    TELNETing to one another.

1. Command name and code

    TUID   26

2. Command Meanings

    IAC WILL TUID

       The sender (the TELNET user) proposes to authenticate the user and
       send the identifing UUID; or, the sender (the TELNET user) agrees
       to authenticate the user on whose behalf the connection is
       initiated.

    IAC WON'T TUID

       The sender (the TELNET user) refuses to authenticate the user on
       whose behalf the connection is initiated.

    IAC DO TUID

       The sender (the TELNET server) proposes that the recipient (the
       TELNET user) authenticate the user and send the identifing UUID;
       or, the sender (the TELNET server) agrees to accept the
       recipient's (the TELNET user's) authentication of the user
       identified by his UUID.

Anderson   [Page 1]

      IAC DON'T TUID

         The sender (the TELNET server) refuses to accept the recipient's
         (the TELNET user) authentication of the user.

      IAC SB TUID <uuid> IAC SE

         The sender (the TELNET user) sends the UUID <uuid> of the user on
         whose behalf the connection is established to the host to which he
         is connected. The <uuid> is a 32 bit binary number.

3. Default

   WON'T TUID

      A TELNET user host (the initiator of a TELNET connection) not
      implementing or using the TUID option will reply WON'T TUID to a
      DO TUID.

   DON'T TUID

      A TELNET server host (the recipient of a TELNET connection) not
      implementing or using the TUID option reply DON'T TUID to a WILL
      TUID.

4. Motivation for the Option

   Under TACACS (the TAC Access Control System) a user must be
   authenticated (give a correct name/password pair) to a TAC before he
   can connect to a host via the TAC. To avoid a second authentication
   by the target host, the TAC can pass along the user's proven identity
   (his UUID) to the that host. Hosts may accept the TAC's
   authentication of the user or not, at their option.

   The same option can be used between any pair of cooperating hosts for
   the purpose of double login avoidance.

5. Description for the Option

   At the time that a host establishes a TELNET connection for a user to
   another host, if the latter supports the TUID option and wants to
   receive the user's UUID, it sends an IAC DO TUID to the the user's
   host. If the user's host supports the TUID option and wants to
   authenticate the user by sending the user's UUID, it responds IAC
   WILL TUID; otherwise it responds with IAC WON'T TUID. If both the
   user and server TELNETs agree, the user TELNET will then send the
   UUID to the server TELNET by sub-negotiation.

6. Examples

   There are two possible negotiations that result in the double login
   avoidance authentication of a user. Both the server and the user
   TELNET support the TUID option.

      S = Server, U = User

      Case 1:

         S-> IAC DO TUID
         U-> IAC WILL TUID
         U-> IAC SB TUID <32-bit UUID> IAC SE

      Case 2:

         U-> IAC WILL TUID
         S-> IAC DO TUID
         U-> IAC SB TUID <32-bit UUID> IAC SE

   There are also two possible negoitiations that do not result in the
   authentication of a user. In the first example the server supports
   TUID and the user TELNET doesn't. In the second example the user
   TELNET supports TUID but the server TELNET doesn't.

      S = Server, U = User

      Case 3:

         S-> IAC DO TUID
         U-> IAC WONT TUID

      Case 4:

         U-> IAC WILL TUID
         S-> IAC DONT TUID

   The TUID is transmitted with the subnegotiation command. For
   example, if the UUID had the value 1 the following string of octets
   would be transmitted:

      IAC SB TUID 0 0 0 1 IAC SE

   If the UUID had the value 255 the following string of octets would be
   transmitted:

      IAC SB TUID 0 0 0 IAC IAC IAC SE

     If the UUID had the value of all ones the following string of octets
     would be transmitted:

        IAC SB TUID IAC IAC IAC IAC IAC IAC IAC IAC IAC SE