Password Generator Protocol

STATUS OF THIS MEMO

   This RFC specifies a standard for the ARPA Internet community. Hosts
   on the ARPA Internet that choose to implement a Password Generator
   Protocol (PWDGEN) are expected to adopt and implement this standard.
   Distribution of this memo is unlimited.

BACKGROUND

   Many security-conscious host administrators are becoming increasingly
   aware that user-selected login passwords are too easy to guess for
   even casual penetration attempts. Some sites have implemented
   dictionary lookup techniques in their password programs to prevent
   ordinary words from being used. Others have implemented some variant
   of a randomly generated password with mixed success. The problem
   arises from the fact that such passwords are difficult to remember
   because they cannot be pronounced or are based on a relatively short
   cycle pseudo-random number generator.

   A version of the PWDGEN algorithm briefly described below has been in
   use for several years at a small number of sites in the Internet.
   Interest has recently been expressed at porting this algorithm to
   other sites. However, the relatively short cycle and the resulting
   randomness of the pseudo-random number generator available on these
   sites tends to interfere with the intended result of minimizing the
   potential duplication of passwords both within a site and across
   sites when a user has access to more than one site.

   The PWDGEN Service described herein provides a means for sites to
   offer a list of possible passwords for the user to choose one from
   the first set, or optionally select from another set. With more than
   one site offering this service, it is then possible to randomly
   select which site to use and have multiple fallback sites should that
   site be unavailable.

   Description

      The PWDGEN Service provides a set of six randomly generated
      eight-character CRLF-delimited "words" with a reasonable level of
      pronounceability, using a multi-level algorithm. An
      implementation of the algorithm is available in FORTRAN-77 for
      examination and possible implementation by system administrators
      only.

The uniqueness of the generated words is highly dependent on the
randomness of the initial seed value used. The availability of a
single system-wide seed, updated after each access is highly
desireable. Seeds based on a time-of-day clock are unacceptable.
Seed values should be stored as values in excess of 32 bits for
best performance.

TCP Based PWDGEN Service

One PWDGEN service is defined as a connection based application on
TCP. A server listens for TCP connections on TCP port 129. Once
a connection is established, the six CRLF-delimited words are
generated and sent to the caller, and the connection is closed by
the server. No dialog is used or required.

UDP Based PWDGEN Service

Another possible PWDGEN service is defined as a datagram based
application on UDP. A server listens for UDP datagrams on UDP
port 129. When a datagram is received, the six CRLF-delimited
words are sent back in an answering datagram.