****

DDN Security Bulletin 04 DCA DDN Defense Communications System
23 Oct 89 Published by: DDN Security Coordination Center
(SCC@NIC.DDN.MIL) (800) 235-3155

DEFENSE DATA NETWORK SECURITY BULLETIN

The DDN SECURITY BULLETIN is distributed by the DDN SCC (Security Coordination Center) under DCA contract as a means of communicating information on network and host security exposures, fixes, & concerns to security & management personnel at DDN facilities. Back issues may be obtained via FTP (or Kermit) from NIC.DDN.MIL [26.0.0.73 or 10.0.0.51] using login="anonymous" and password="guest". The bulletin pathname is SCC:DDN-SECURITY-nn (where "nn" is the bulletin number).

****

HALLOWEEN PRECAUTIONARY NOTE

Halloween is traditionally a time for tricks of all kinds. In order to guard against possible benign or malevolent attempts to affect the normal operation of your host, the DDN SCC staff suggests taking the following easy precautions:

1. Write a set of emergency procedures for your site and keep it up to date. Address such things as:

   - What would you do if you had an intruder (either a human or a computer virus)?

   - Who would you call for help? HINT: Read the top of this bulletin! Also, for 24 hour assistance:

     MILNET Trouble Desk -- (A/V) 231-1713 or (800) 451-7413

   - Who is in charge of security at your site?

   - How would you apply a hardware/software fix if needed?

2. Save your files regularly, and make file back-ups often. Put the distribution copies of your software in a safe place away from your computer room. Don't forget where they're stored!

3. Avoid trivial passwords and change them often. (See the "Green Book" (Department of Defense Password Management Guideline), CSC-STD-002-85, for information on the use of passwords.)

4. Check to make sure your host has no unauthorized users or accounts. Also check for obsolete accounts (a favorite path for intruders to gain access).

5. Restrict system ("superuser", "maint", etc.) privileges to the minimum number of accounts you possibly can.

6. Well publicized accounts including "root", "guest", etc. AND the personal account for the system administrator should NOT have system privileges. (Past experience has shown that these IDs are more susceptible to successful intruder attacks.)

7. Keep your maintenance contracts active.

Of course, these steps should be taken throughout the year as part of your regular operating procedure.

****