UNIXG: New password security software

Satnam Purewal
satnam.purewal@ubc.ca

On November 22, University Computing Services staff added password checking software to UNIXG to help ensure the system's security.

Password checking software is rapidly becoming a common feature of North American UNIX systems. It requires passwords to meet strict guidelines for complexity. Passwords must be six to eight characters long, contain a sufficient mix of upper- and lower-case letters, numbers and punctuation and not be found in a special on-line "dictionary," which is not a published English dictionary but an extensive listing of common letter and number patterns, specialized vocabulary, abbreviations and names as well as words.

Creating a complex password

The checking software weighs various factors before it accepts your new password. If your password is complex enough (containing punctuation and numbers), you may be able to use only six characters; if your password contains only lower case letters, you will need to use the full eight characters allowed.

Creating a password that you can remember easily, but that will pass the checking software, may require more than one try. A good method is to combine two or more short misspelled words with punctuation, upper-case letters or numbers. Or try substituting some punctuation or numbers for a couple of letters in an eight-letter word that you will remember. You can invent an eight word sentence and use the initial letters from each word, mixing upper- and lower-case letters and substituting a number for at least one letter. Try to make your password complex in more than one way (for example, not just long, but containing several different kinds of characters).

System security

Secure passwords are an important part of any system's security. In the last few months a number of UNIX system administrators in North America have reported unauthorized use of their systems. When unauthorized users crack a system every user's files are threatened, not just those of the user whose password was cracked to gain entry. In some cases the entire system may go down for a period of time.

In a recent incident, an Ontario university's system was cracked and files from that university's system were moved by the cracker. The unauthorized entry was traced to a UNIXG account belonging to a UBC student who had e-mailed his ID and password to a friend at another university. The cracker was monitoring e-mail messages at that university, found and read the UBC student's message, and appropriated the UNIXG account, using it to crack the Ontario university's system behind the mask of a UBC identity. This example demonstrates that the presence of crackers on a system jeopardizes everyone's privacy. If you reveal your password or have a crackable password, you could be held responsible for system damages done by someone else using your account to gain entry to other systems in other provinces or countries.

All UNIXG users were asked to change their passwords before December 6, in order to implement the greater security protection made possible by the new software. Users who did not change their passwords had their accounts temporarily disabled and were asked to contact the C&C Computer Accounts office to have their accounts enabled again. This security check is another way to ensure that accounts are being used only by their authorized users. Computing and Communications is grateful to all UNIXG users for their cooperation during this period.

when unauthorized users crack a system every user's files are threatened

If you suspect that your account has been used by someone else, please report the event to Satnam Purewal at **satnam.purewal@ubc.ca** or by telephone at 822-4820.❑