

BDM INFORMATION SYSTEMS

BDM Biometric Security

Application Note

PASSWORDS THE WEAKEST LINK



The challenge for pharmacy administration management in protecting patient privacy continues to be network protection and the vulnerabilities in pharmacy information management systems. Recently a regional health care company had Neohapsis, a Chicago-based security company look for security holes in their network system. To test the network system, Neohapsis used “John the Ripper” a well known cracking program to find any security problems. Normally well-chosen passwords could take years, if not decades of computer time to crack. It took the program only an hour to decipher 30 percent of the passwords for nearly 10,000 accounts listed in the password file.

“Just about every company that we have gone into, even large multinationals, has a high percentage of accounts with easily cracked passwords,” said Greg Shipley, Director of Consulting for Neohapsis. “We have yet to see a company whose employees don’t pick bad passwords.”

Fortune 100 corporations, small firms and even Internet service providers with strong security have an Achilles heel if their users pick easily guessable passwords. Some choose words straight out of Webster’s dictionary, others use a pet’s name. Many who think themselves tricky append a digit or two on the end of their chosen word. Such feeble attempts at deception are no match for today’s computers, which are capable of trying millions of word variations per second and often can guess a good number of passwords in less than a minute.

An eight-character password can be very secure, even if attacked by today’s high-speed computers. There are more than 6.6 quadrillion different eight-character passwords using the 95 printable ASCII characters. Though some password-cracking programs can test nearly 8 million combinations every second on the latest Pentium 4 processor, breaking an eight-character password would still take more than 13 years on average.

Even the most paranoid security group and high-tech digital fences can’t do much if the CEO secures their critical files with “god123.” Worst, most companies and organizations still rely on a password, and nothing else to authenticate their employees. A good defense is to make passwords nearly impossible to guess, but such strength requires that the password be selected in a totally random fashion. That’s a tall order for humans, said David Evans, an assistant professor of computer science at the University of Virginia. “When humans make passwords, they are not very good at making up randomness,” he said.



BDM INFORMATION SYSTEMS

BDM Biometric Security

Application Note

Furthermore, because people usually have several passwords to keep track of, locking user accounts with random, but difficult-to-remember, strings of characters such as “wX595qd!” is a recipe for a support headache. “The idea is to make something that is easy to remember but that will make up a good password,” he said.

Many security administrators focus their efforts on teaching users how to use various mnemonics to create strong, but memorable, passwords. A common technique takes the first or last letter of each word in a saying or phrase familiar to the user. For example, by random capitalization and substituting some punctuation marks and digits for letters, “Friends don’t let friends give tech advice” might become “fD!Fg7a.” Unfortunately the education does not seem to be sticking, and the password problem is getting worse as the percentage of less-tech-savvy computer users increases.

“The human limitation with precise recall is in direct conflict with the requirements of strong passwords,” wrote University of California at Berkeley Rachna Dhamija and Adrian Perrig in a recent paper. Researchers at Microsoft, Lucent Technologies, New York University and the University of Virginia, among others, have studied techniques for creating graphical passwords. Such systems have problems as well. “Pictures are going to be easier to shoulder-surf than keyboard passwords,” said Chris Wysopal, director of research and development for digital security firm Stake, adding that weaknesses in how such passwords are stored on the computer system could also make them vulnerable to cracking attempts.



“If you want real high-level security,” said University of Virginia’s David Evans, “people can authenticate themselves with something they know, like a password; something they have, like a smart card; and something they are, like a biometric.”

Fingerprint scanners and smart-card readers are still not a common option on computers, said Chris Christiansen, an analyst with market researcher IDC. “There is a huge, huge range of alternatives to passwords,” he said.

Passwords will continue to be the greatest vulnerability faced by pharmacy administrators to create secure pharmacy networks. **BDM BIOMETRIC SECURITY** offers a better alternative to the RxTFC® user.

BDM BIOMETRIC SECURITY is an option that is available to users of **RxTFC® PHARMACY INFORMATION SYSTEMS**. To ease password management and improve the security of your pharmacy network give your **BDM** sales representative a call today!

DON'T USE DICTIONARY WORDS

Webster’s New World College Dictionary has 163,000 words in it. The smallest dictionary in a password cracker has more than 200,000, including places and popular names such as Spock.

DON'T USE PERSONAL INFORMATION

Social security numbers telephone numbers, date of birth, and the names of children, pets and significant others should all be considered off limits.

DON'T GIVE YOUR PASSWORD OUT TO ANYONE

No one, not even the system administrator, needs your password. If someone asks for your password, assume the worst.

DO USE A DIFFERENT PASSWORD ON EACH IMPORTANT SYSTEM

Assume that the administrator for each system can decipher your password for that system. Don’t give them access to all of your accounts. By using different passwords, you limit the damage of a breach to a single account.

DO USE NUMBERS AND SYMBOLS, AND NOT JUST AT THE END

There are several good mnemonics for generating passwords. Use the first letter of each word in a sentence and then randomly capitalize some letters and add numbers and special characters.