Just Say No to Passwords!

BY JOHN E. JOHNSTON

I really feel sorry for the users in my organization. I work in a hospital, and doctors, nurses, and other medical professionals must use the systems we provide them. These medical people would rather (and should rather) concentrate on medical problems than deal with computer problems. Yet the way we deliver applications forces them to deal with computer problems more often than necessary.

Let me explain what I mean: A typical Windows 95 workstation that we have deployed on a nursing unit has access to the following computing platforms:

- IBM mainframe
- NetWare 4.x servers
- NetWare 3.x servers
- Windows NT servers
- Multiple DEC/VAX systems
- UNIX machines
- AS/400

Each of these platforms requires a userid and password. We try to keep the userid the same on each platform, but keeping the passwords in sync with each other is almost impossible. The mainframe password expires every 90 days, and the user must then select a new one. The NetWare passwords also expire every 90 days but never in sync with the mainframe. The NT passwords never expire and the DEC passwords expire every 60 days.

Running on each of these platforms are multiple applications. A typical nursing PC can access up to 20 major applications, and most of these also have their own userids and passwords. Again, we try to keep the userid consistent across all platforms and applications, but this is not always possible. Would you believe we have one application that requires a two-byte userid? Keeping the applications passwords in sync with the platform passwords is also a loosing battle. So now, the user has to remember multiple userids and multiple passwords.

I then realized that our environment is obviously not secure with all these layers of userids and passwords, so why are we putting our users through this hassle? I could think of no good reason.

We all thought that this setup, albeit a bit cumbersome, was very secure. Nobody can hack our systems! Well let me tell you a short story: A few weeks ago, my group implemented a large software upgrade that required us to visit each PC on the nursing units to modify some settings. In all, we visited about 130 PCs. Part of the software upgrade process required re-booting of the PC. Many times, the user was unavailable when we re-booted. When the PC prompted us for passwords, and the user was nowhere in sight, we started snooping. Many times we would look under the keyboard and find a piece of paper with all of the userids and passwords listed on it. Other times, the userid and password were written on a Post-It note stuck right on the monitor. Some users simply wrote their userids and passwords right on the PC. Of the 130 PCs we visited, we only had to ask a handful of users for their password, the rest we hacked (if you could call such simple snooping hacking).

I then realized that our environment is obviously not secure with all these layers of userids and passwords, so why are we putting our users through this hassle? I could think of no good reason.

So, my group did a bit of brainstorming and came up with an idea. Each PC and printer has an asset tag stuck to it. This tag consists of a five-digit number. Why not have the user simply enter this number when they login to our systems? We figured we would put a "U" in front of the tag number for the userid, and use the tag number itself as the password. For example, if the asset tag for a PC was 01235, the user would login using a userid of U01235 and a password of 01235. We would use Windows 95 profiles along with NetWare security to determine which applications the U01235 user could access. Printer queues would also be named after the tag number; for example, P01236 would be the print queue name for the printer with tag number 01236. We would also change all the platform and application userids and passwords to match this new standard (where possible). Let's look at the positive aspects to this approach:

- less user frustration
- simpler network administration
- easier to tell which print queue is associated with a printer
- reduced number of help desk calls

The negatives that I know of include:

- difficulty keeping email secured (if email is given to all users)
- easy for someone to snoop around on different PCs (within the organization)

This approach may work well for groups of users, such as nurses and transcriptionists, but there are some users who, because of their access to secure data, require a unique userid and a secure password. For these users we again utilize Window 95 profiles. Using these profiles, secured users can logon to any PC in the organization and get their own customized desktop and security rights.

Remote access is another story altogether. None of the generic userids would be allowed to access the network from a remote (dial-up) connection. All users who must access the network via dial-up will be required to have a unique userid and a secured password.

When a PC is replaced with a newer model, the asset tag will be removed from the old PC and placed on the new PC. This will prevent us from having to rename the userids and change the passwords. When a new PC or printer is installed, we simply change our asset database to reflect the hardware change.

Will we be less secure with this method than with the old method? Maybe a bit. Would it be worth the risk to alleviate so many problems? In my opinion, yes. If any of you have had similar problems with multiple userids and passwords, please email your comments to editor@naspa.net or me at johnj@fast.net. We will publish your ideas in upcoming issues of ***Technical Support***. Also, if you have any ideas for future topics for this column, please contact me. *ts*

NaSPA member John E. Johnston is manager of technical support and communications for a major hospital in Pennsylvania. He designs and maintains cross-platform local and wide area networks utilizing NetWare, OS/2, DOS, and Windows.