I'm no genius, but let me ask 10 of your company's network users a few personal questions, and I'm willing to bet that I can guess at least seven of their passwords. Even if I have a bad day and can guess only one password, your company's network security is easily compromised.

Why are passwords so easy to guess? As you know only too well, remembering all of the passwords you rely on to access the many secure applications you use daily is difficult. For example, you log in to the network, check your e-mail messages, maybe log in to your bank's web site to see how much money you have, access a mainframe application, access a UNIX server, and so on all day long. In the name of security, almost everything you do is password protected.

This quest for tight security is creating a security risk all its own: Because users have so many different passwords to remember, they choose passwords that are easy to remember. For example, they may use their spouse's, pet's, or child's name followed by the month. Are your company's secrets protected by "billy12"?

To solve the issue of multiple passwords, you may want to consider a single sign-on application such as SecureLogin from Protocom Development Systems. With SecureLogin, users have to remember only one password, and SecureLogin secures their other passwords and automatically supplies these passwords when the users log in to password-protected applications.

Because users need to remember only one password, they can make this password a unique combination of alpha and numeric characters—making the password significantly more difficult to crack. To further protect your company's network, you can also use SecureLogin with biometric or smart card devices.

THE BASICS OF SECURELOGIN

Because SecureLogin has been around since 1994, the product has matured considerably over the years. SecureLogin now supports nearly every major front-end and back-end platform.

For example, SecureLogin supports workstations running Windows 2000, ME, NT 4.0, 98, and 95.

On the back-end, SecureLogin supports NDS eDirectory, Active Directory, and Lightweight Directory Access Protocol (LDAP). SecureLogin also supports Windows NT Server 4.0; NetWare 5, 4, and 3; Solaris 2.6 and above; and Linux. (For a list of products and industry-standard technologies that SecureLogin supports, see "Supporting Cast" on p. 48.)

By supporting a variety of platforms, SecureLogin allows you to manage your company's heterogeneous environment. No matter what platforms your company uses, you can use one single sign-on product.

SecureLogin extends the NDS schema to accommodate authentication data, such as usernames and passwords. As the network administrator, you must extend the NDS schema the first time you install SecureLogin. After the NDS schema is extended, users can install SecureLogin on their own workstation.

SecureLogin stores this authentication data in encrypted form within individual User objects. As a result, when a user logs in to NDS eDirectory, SecureLogin can access stored usernames and passwords, enabling SecureLogin to transparently log users into other applications. In addition, SecureLogin can take advantage of all the fault-tolerant and replication features of NDS eDirectory.

SecureLogin uses the following two methods to authenticate users to applications:

- **Background Authentication.** Based on the mainframe pass- 
ticket system, Background Authentication uses dynamic passwords that change each time the user accesses an application. (A pass ticket is a password that is valid only for a specified amount of time.) SecureLogin uses a pass ticket that is valid for only 30 seconds. Each pass ticket is generated based on a set of specific criteria. For example, SecureLogin uses a pass ticket that is based on the time the pass ticket is issued and a key that is unique for each user.
SecureLogin uses a triple Data Encryption Standard (DES) algorithm to generate a challenge and response between the client and the device the user is attempting to access. This challenge-and-response method requires the application to have a plug-in module, which interprets the pass ticket. If no module exists or can be written for a particular application, you can use the more common password store-and-forward method.

- **Password Store-and-Forward.** Also called the username/password replay mode, Password Store-and-Forward allows SecureLogin to support applications that do not have a plug-in module for Background Authentication. In addition to using SecureLogin to access applications, users can use SecureLogin to provide single sign-on to a Windows dialog box, an HTML interface, a mainframe, or a UNIX session.

  With Password Store-and-Forward, workstation agents capture the username and password that a user enters the first time he or she accesses an application. (Workstation agents are installed when you install SecureLogin.) These agents store the username and password in NDS eDirectory and replay this information when the user accesses the application. (For complex logon sequences, SecureLogin also supports scripts, which are explained later in this article.)

**Figure 1.** Users can use SecureLogin to automatically authenticate to their favorite web sites.

For more information, visit www.ncmag.com/advertise.html.

IMPLEMENTING SECURELOGIN

SecureLogin ships on a CD, which you use to install the application on a Windows workstation. When you launch the installation program, SecureLogin prompts you for a password (which Protocoom provides after purchase) that unlocks the program. After you enter this password, you select the platform on which you want to store SecureLogin information. For example, you can choose Standalone, NDS eDirectory, Active Directory, Windows NT 4 Domains, or Windows NT 4 Terminal Server. For this review, I chose to install SecureLogin on NDS eDirectory.

You must then select which components you want to use to manage SecureLogin and which applications you want to work with SecureLogin. For example, you can choose components such as the NetWare Administrator (N W A D M I N ) snap-in modules or extensions for applications such as Internet Explorer, Netscape Navigator, and Lotus Notes.

Next, you or the user must configure SecureLogin by actually logging in to applications and having SecureLogin capture and store the login information that is entered. After installation, SecureLogin loads a workstation agent that appears in the taskbar of the Windows desktop. SecureLogin then waits for the user to log in to an application that requires authentication.

HOW SECURE CAN YOUR COMPANY BE?

Whichever authentication method you use for your company, users will not know the difference: Users will simply log in to NDS eDirectory and transparently access all of the applications to which they have been given rights.

Single sign-on benefits both your company's users and you as the network administrator: Users will no longer need to remember multiple usernames and passwords, and you will not have to reset passwords when users predictably forget their original passwords.

However, single sign-on magnifies the importance of ensuring that users are who they say they are during the initial login. You can increase the likelihood that users are who they say they are by using high-security products such as biometric logins, smart cards, and tokens. SecureLogin supports all of these types of login methods.

For example, I tested SecuGen Corp.'s EyeD Mouse, a fingerprint-reading mouse, with SecureLogin. To use the EyeD Mouse, you press your thumb on the mouse, and it identifies who you are and logs you in to the network. This type of biometric login is quite a bit more secure than entering "billy12" as your password for the month. (For more information about SecuGen, visit www.sccugen.com.)

Note. You can disable this icon so that users don't even know SecureLogin is installed on their workstation.

Simple Login Sequences

When a user logs in to an application that is not yet registered with SecureLogin, a wizard pops up. This wizard allows the user to easily define the login fields, such as the username and password fields, as well as any other fields the application requires.

To find out how SecureLogin works, I launched my browser and went to PayPal, an online payment system that requires authentication. As soon as PayPal presented me with a login prompt, SecureLogin opened a dialog box, asking if I wanted to have SecureLogin remember the login information so it could log me in automatically in the future. (See Figure 1 on p. 45.) I simply clicked "Yes," and the next time I visited PayPal, SecureLogin automatically logged me in.

Complex Logon Sequences

If users must access an application or device that has a complex logon sequence (such as logon sequence for a mainframe), you can use the scripting tool included with SecureLogin to enable single sign-on. You can also use this scripting tool to enable users to log in to an application and proceed to a specific portion of that application.

For example, if you need to work in only one portion of the mainframe and do not want to have to "walk" the menus to access the information you need, you can use SecureLogin to simplify your login: You simply create a SecureLogin script, and when you click on the mainframe icon on your Windows desktop, SecureLogin takes you right to the spot where you work. (Despite the similarity in names, SecureLogin scripts should not be confused with NetWare's login scripts.)

To create SecureLogin scripts such as these, you first double-click the SecureLogin icon in your Windows taskbar and select the scripting tool. The scripting tool supports the use of variables, including NDS names. For example, %CN stands for the user's common name, %lastname stands for the user's last name, and so on.

The SecureLogin scripting tool also enables you to insert specific information that is stored in NDS eDirectory into a
mainframe, Windows, or HTML field. For example, you can create a SecureLogin script that limits the amount of information a user is prompted for the first time he or she uses SecureLogin. The user enters the information, clicks OK, and the process is completed. This feature is handy if you are rolling out a new application or providing access to new users.

You can also use the SecureLogin scripting tool to build customized dialog boxes. For example, if you need a dialog box to say something other than what is included in the existing background authentication wizard box, you can change that box to meet your needs.

The scripting tool also enables you to establish rules regarding field length, acceptable characters, and so on. You can also create scripts for applications that require users to change passwords frequently. When the password expires, SecureLogin automatically changes the password. As a result, users will never be prompted again for a new password.

NOW YOU SEE IT, NOW YOU DON’T
You can make SecureLogin invisible to users while retaining all of your configuration options. For example, you can decide what you want to allow certain users or groups to be able to do. You can prevent users from adding passwords for applications they access for personal use, such as their investing, banking, or other password-protected web applications. By forcing users to log on manually, you will eliminate help-desk calls for login issues for personal applications.

As mentioned previously, you can use the NWADMIN utility to configure SecureLogin. (See Figure 2.) In addition, you do not need ADMIN-security equivalence to manage SecureLogin. For example, you can delegate SecureLogin management to the security department. Because all of the username and password data for SecureLogin is encrypted and stored inside NDS eDirectory, even the network administrator cannot access the passwords.

SecureLogin also has built-in Simple Network Management Protocol (SNMP) capabilities so that you can monitor the use of password-protected applications and then generate reports. When a user uses SecureLogin, the application generates an SNMP trap, which enables you to track how often SecureLogin is used, how long it is used, and how long it takes to log in to the application. You can then build metrics over time to know how well your company's network is performing and what effect SecureLogin events have on your company's network.

In addition, you can enable an SNMP option during the SecureLogin installation. If this option is enabled, SecureLogin will generate an SNMP trap if a particular dialog box appears or if a particular piece of text on a mainframe screen appears. For example, if the wrong password is entered, the resulting dialog box that appears will trigger an SNMP trap. SecureLogin will then send an alert to the management console.

SECURE SCREEN LOCK
To maintain a secure environment, you need the ability to conveniently


For more information, visit www.ncmag.com/advertise.html.
secure your desktop when you are away. SecureLogin includes a secure screen saver that goes beyond Windows’ ability to password-protect the screen saver. SecureLogin’s screen saver offers the following benefits:

- The ability to automatically log off of the network if the workstation has been unattended for a specified period of time
- The ability to use smart cards and biometric logins, as well as the network password
- The ability to rotate graphics used in the screen saver
- The ability to put the mouse in a corner of the screen to lock it immediately through the use of hotspot activation

USING CITRIX AND TERMINAL SERVER

SecureLogin offers special support for Citrix and Windows NT Terminal Server, allowing you to integrate SecureLogin in this type of environment. If multiple users share a single PC, you can have multiple secured sessions. Each session is independent of the other sessions, and each session can be secured using the screen-lock feature.

If the screen lock has been enabled on a PC, a user simply puts his or her finger on the biometric mouse (or enters a password). This action unlocks the screen and begins the user’s session on that PC. When the user’s session is completed, the user simply relocks the screen. The next user simply puts his or her finger on the mouse (or enters a password) to unlock his or her session.

Citrix and Windows NT Terminal Server maintain the different user sessions, but SecureLogin makes it easier for users to begin and end their sessions while keeping each session secure.

IS SINGLE SIGN-ON WORTH THE COST?

SecureLogin saves money by reducing the number of calls users make to company help desks asking for password resets. In fact, these types of calls will dramatically decrease or disappear altogether. For example, if you use Background Authentication, you will not have to reset passwords because the password exchange is encrypted.

For companies with high-security demands, such as companies that have legal requirements for security, you will probably use SecureLogin’s Background Authentication in conjunction with verification technologies such as biometric methods, smart cards, or tokens. These products and technologies add to the cost of SecureLogin’s implementation. However, these products and technologies also provide an incredibly secure environment while providing easy access to all the applications users need—and of course, to which users have access rights.

CONCLUSION

Logging in to your company’s network and applications needs to be more secure than just an easily guessed password. SecureLogin provides a complete user authentication environment that ensures that users logging in are who they say they are. SecureLogin removes the complexity of logging in to multiple systems and applications: A user needs to remember only one password. As a result, SecureLogin helps reduce or even eliminate password-related calls to help desk.

I like SecureLogin and recommend it for companies that require tight security or require users to access multiple password-protected applications. SecureLogin is the ideal single sign-on solution for heterogeneous networks. In addition, SecureLogin has been Novell Yes, Tested and Approved, making it an ideal solution for Novell networks.

Dennis Williams is director of ProductReviews.com, an Internet site specializing in networking product reviews and product improvement consulting. You can reach him at Dennis@ProductReviews.com.