

MAKING SURE
YOU SECURE
THE DOOR

BY JEFFREY
HARRIS

PHOTOGRAPH
BY HOLLY
LINDEM



Who are you? Well, in a digital world you're typically a username and a password. These form the doorway to your digital identity. Unfortunately, on the Net you can quickly end up with a whole lot of "doorways" into your digital world based on your interactions. Bank identity, airline identity, eBay identity, and on and on. Couple that with work-related network and applications access and there are likely a whole lot of digital You's out there in cyberspace.

And if you also happen to be a network administrator, you get to worry not only about all your own digital doorways, but also about all your users' doorways. How users manage digital doorways to identity directly affects the security of your critical business systems. Do they write down passwords? Store them in PDAs? Use the same password everywhere? Use their pet's

name? More often than not, if they're like the rest of us, this is the case. These practices reduce the effectiveness of your network security—and password policies that require stronger passwords and more frequent changes may actually exacerbate the problem!

There's not only a security angle to this problem, but also a financial one. You and your users have to keep all those digital doorways straight. And unfortunately, each doorway has its own lock, each with its own username and password rules: password length, use of special characters and/or numbers, how often the password must be reset, and rules for password reuse. All of these add complexity to your users' security environment that will regularly have them forgetting passwords—and calling you for help!

Some studies have found that up to 30 percent of help desk calls result from password-related issues and that each time end

NOVELL SECURELOGIN: HOW IT WORKS

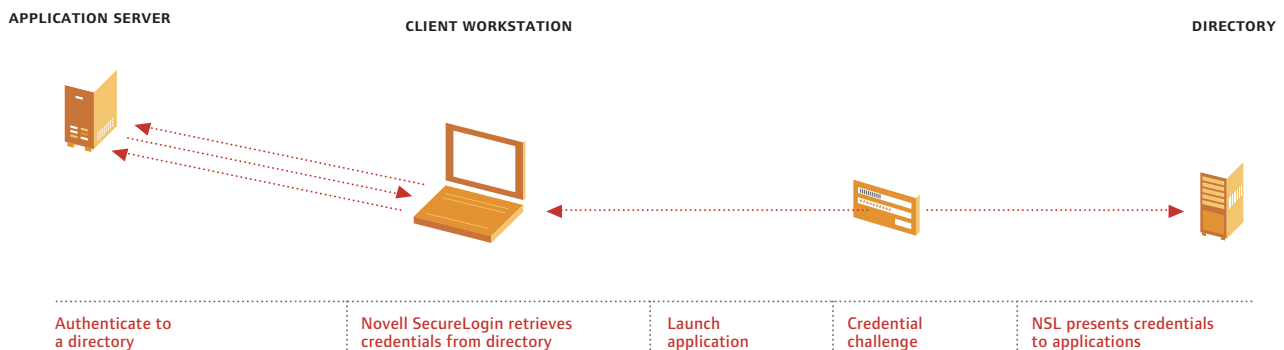


FIGURE 1

Some studies have found that up to 30 percent of help desk calls result from password-related issues and that each time end users call the help desk, it can cost up to \$50.

users call the help desk, it can cost up to \$50. From there you can do the math and see that the complexity of today's digital doorways are costing your organization money, potentially lots of it!

Fortunately, this problem is one of the "low hanging fruit" with Novell Nsure SecureLogin 3.5. (For more information, see www.novell.com/securelogin.) "Password management functions will continue to be used in help desk environments, but the end of 2003 will find most enterprise password management deployments placed within administrative capabilities, incorporated into identity management-related products such as provisioning, Web single sign-on and portals." (2002, Giga Information Group.)

DIRECTORY-ENABLING YOUR PASSWORDS

Basically, SecureLogin creates a secure storage point for all the credentials (usernames and passwords) you need to get through each of your digital doorways. (See Figure 1.) This storage point can be located in any LDAP v3 directory, although using Novell eDirectory adds the advantage of integration with Novell's patented SecretStore technology. (For more information, see *The Ultimate Directory Lockbox*, on this page.) You remember only the credentials to your primary doorway—the directory—and SecureLogin handles the rest. When you access an application or secure Web site, SecureLogin automatically delivers your unique credentials for that particular site from your directory repository.

SecureLogin is a password management solution, not a password synchronization tool. This means that you don't have to drop to the lowest common denominator in order to get a single sign-on solution. Each credential managed by SecureLogin is encrypted with its own unique key using 168-bit 3DES (Triple DES) cryptography, which is a symmetric cryptographic algorithm based on the U.S. government's Data Encryption Standard (DES). It uses a single 168-bit key for both encrypting and decrypting messages.

But what about mobile users? SecureLogin has you covered by allowing you to copy your secure credential repository, again using 168-bit 3DES encryption, to your local machine so that single sign-on works even when you don't have access to the directory in which your SecureLogin secrets are stored. Not only

The Ultimate Directory Lockbox

When you use Novell Nsure SecureLogin with Novell eDirectory, you get the added advantage of an exceptional storage place for the keys to all your "digital doorways."

Novell SecretStore is an eDirectory-based infrastructure in which applications and services may store user authentication secrets. SecretStore is a key component of the Novell secure identity management architecture.

SecretStore automatically determines and leverages the highest level of cryptographic security available for both storage of authentication secrets and transmission of those secrets between eDirectory and the designated application.

To simplify the integration of external applications and services, SecretStore provides Universal Connectors that automatically intercept any prompt for authentication and then interact with the user to collect credentials and securely lock them away. Universal Connectors make it possible to provide single sign-on to an application without modifications to the application code itself.

SecureLogin leverages the universal connector capabilities of SecretStore when used with eDirectory. SecureLogin relies on the individual application, including Windows, Web browsers, and terminal emulators, to recognize a prompt for authentication. It integrates with the authentication process through the SecureLogin Wizard or an existing script.

FOR MORE DETAILED INFORMATION ON SECRETSTORE, CHECK OUT THE ARTICLE IN THE MAY 2003 ISSUE OF NOVELL APPNOTES AT www.developer.novell.com/research/appnotes/2003/a0305.htm.

Letting Novell help you put it all together

If you are like me, sometimes the complexity of today's secure network solutions is enough to make your head swim. It's times like this when Novell Ngage consulting has the cure for what ails you.

Implementing a secure identity management solution such as Novell Nsure SecureLogin requires more than just installing an app and turning it on. A true solution integrates with existing infrastructure investments, supports your business goals and leaves the door open for future adaptation as your business environment evolves.

Novell consulting delivers true solutions through a combination of practical business knowledge, professional consulting background and a deep technical expertise. Not only that, but Novell delivers world-class support and training offerings to provide all the resources you need to receive the maximum benefit from your investments.

After all, SecureLogin isn't the whole story when it comes to network security—it's an important component of a broader strategy to protect your organization's valuable assets and improve the productivity of your employees. Novell consulting can help you define and support a broad security strategy as you look to implement SecureLogin by helping you with the following:

- Develop an understanding of the "bigger picture" of network security and how SecureLogin supports security goals.
- Analyze existing helpdesk costs and develop an accurate ROI estimate for implementing SecureLogin as well as tracking the results to prove out the savings.
- Develop a streamlined authentication process by eliminating repetitive sign on, and develop metrics that let you quantify savings.
- Prioritize the inclusion of applications in a SecureLogin solution based on your organization's business needs.
- Determine business critical applications that would benefit from tighter security, and develop a plan to implement that security within the framework provided by SecureLogin.

Any way you look at it, taking advantage of the Novell consulting in your SecureLogin solution will result in a more effective, and more secure network environment.

that, SecureLogin 3.5 includes a Secure Workstation feature that provides much greater security for notebook computers and the valuable data that road warriors often keep with them.

But doesn't single sign-on just provide a single point of failure? While technically true, this argument is really a red herring. The additional security gained by eliminating poor password habits and user "work arounds" contributes significantly to the overall security of your network. In addition, accessing all your digital

With SecureLogin managing your digital doorways, the strength of the primary authentication is automatically applied to all your business systems, applications and secure Web sites.

doorways through SecureLogin gives you the freedom to greatly increase the security of the primary login. You can require more complex passwords, enforce password changes or even move to more secure authentication methods such as smart cards, tokens or biometrics. With SecureLogin managing your digital doorways, the strength of the primary authentication is automatically applied to all your business systems, applications and secure Web sites.

But how does SecureLogin prevent a rogue administrator from hijacking your credentials? SecureLogin encrypts all credentials stored in the directory, thereby protecting them from direct view. SecureLogin also goes one step further by requiring a user to

provide the old password or answer a challenge question before permitting access to credentials. Similarly, all SecureLogin credentials are locked if an attempt is made to move those credentials to a different user object. Network administrators don't have any more access to your digital doorways than does anyone else.

A CLOSER LOOK AT SECURELOGIN 3.5

SecureLogin 3.5 takes host-based single sign-on to a new level by wrapping a comprehensive security solution around its core single sign-on functionality. The result is a product with everything you need to secure your users' digital doorways, and thereby increase the security of your own business environment.

BROAD APPLICATION SUPPORT:

In order to capture and interact with your applications and secure Web sites to provide single sign-on, SecureLogin must understand how to interact with many different types of application interfaces. With version 3.5, SecureLogin extends its application support to support the broadest range of applications on the market, including:

- Windows 32-bit applications
- Citrix-based applications (thin-client)
- Java applications that leverage Abstract Windows Toolkit (AWT), including Swing GUI development components
- E-mail clients, including Novell GroupWise, Lotus Notes and Microsoft Outlook

- IBM and UNIX mainframe applications
- Remote Authentication Dial-In User Service (RADIUS)-compliant routers
- More than 30 terminal emulators

All this application support means that if you have an application, you can likely manage access to that application with SecureLogin. Gabe Waters, Novell Product Manager for SecureLogin, says "I used to think I had 14 or 15 identities to manage, but once I got working with SecureLogin I quickly found I had nearly 50! There's no way I could keep track of all those credentials effectively and still maintain a secure environment." But SecureLogin can.

Comprehensive Workstation Security:
We all know that securing a user's digital doorways involves more than single sign-on. Single sign-on provides the opportunity to better secure your Net while at the same time improving a user's experience and productivity. As one of the premier network security companies, Novell gets it as well. That's why SecureLogin 3.5 now includes Novell Modular Authentication Services Enterprise Edition (NMAE). (For more information, see www.novell.com/nmas.) NMAE gives you the ability to leverage strong authentication methods to improve your primary authentication process.

NMAE also provides Secure Workstation, a powerful new set of tools for helping users to properly secure their workstations. As with other SecureLogin

www.
caminosoft
.com

Secure Workstation provides a “single click” logout that will gracefully shut down applications, log out the user, and present a new login dialog for the next user.

features, Secure Workstation is available to both connected and disconnected workstations.

Secure Workstation provides a policy-based framework within which you can control locking the workstation and auto-logout of users based upon several different events, such as:

- Period of inactivity (configurable)
- Proximity card removal
- Smart card removal

Furthermore, Secure Workstation provides a “single click” logout that will gracefully shut down applications, log out the user, and present a new login dialog for the next user. This feature is crucial for shared workstations, and is particularly important in light of recent privacy legislation such as HIPAA for healthcare organizations and Gramm-Leach-Bliley for financial services organizations.

Finally, NMAS also provides a feature known as pcProx for SecureLogin. pcProx allows you to require an additional authentication event (directory re-authentication, smart card, biometric, etc.) before SecureLogin will pass its credentials to the user-requested application. This provides yet another level of control over very sensitive applications or systems.

SIMPLE MANAGEMENT TOOLS:

The key to simplifying management is to use the tools that are already there. SecureLogin 3.5 takes this to heart by leveraging the directory-based management tools that are already available wherever possible. If you are an eDirectory shop, SecureLogin is managed through ConsoleOne just like the rest of your environment. If you are an Active Directory shop, SecureLogin provides a snap-in to the Microsoft Management Console (MMC). Finally, if you run a different LDAP directory, or NT Domains, SecureLogin provides its own management console known as SecureLogin Manager.

SecureLogin utilizes a powerful yet easy-to-use scripting language for mapping the login process for an application. The

SecureLogin Wizard typically creates scripts automatically when you select an application for management by SecureLogin. (See Figure 2.) However, network administrators can also manually define application scripts as needed. Script format varies based on application type (Windows, Web, terminal emulator, etc.), thereby providing the maximum possible capability to support the specific authentication features of any given application.

The SecureLogin Wizard typically creates scripts automatically when you select an application for management by SecureLogin. Network admins can also manually define application scripts.

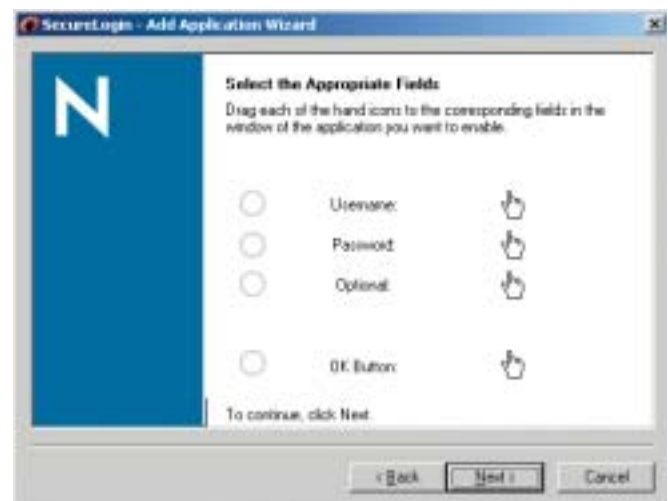


FIGURE 2

SECURING YOUR WORLD

As your digital world continues to increase in complexity, security solutions that are capable of addressing that complexity are becoming increasingly important. You need to protect the security of your environment while simultaneously protecting your organization's bottom line. SecureLogin 3.5 makes this possible. In fact, implementing SecureLogin is the "low hanging fruit" in your battle for network security without increasing costs.

On a personal level, SecureLogin gives network managers a chance to look really good to both your network users and your company execs, and that's a rare and wonderful thing. Consider the following:

- Analyst studies show that the helpdesk in larger organizations with just four to eight separate applications will spend nearly 50 minutes per user per year to address password-related issues. Assuming a helpdesk labor rate of \$18 per hour, a 5000-person organization is looking at \$74,700 in helpdesk costs to address password-related issues.
- Lost productivity is the other part of the equation. Research has found that 70.4 percent of users spend at least 25 minutes per month getting password help. Assuming an average labor rate of \$18 per hour, a 5000-person organization is looking at \$316,800 per year in lost productivity.

- SecureLogin has been proven to eliminate up to 95 percent of an organization's password-related issues. That means that the same 5000-person organization could save \$371,925 in the first year after implementing SecureLogin!
- Users can throw away their sticky notes, forget application passwords and reduce the clutter surrounding their digital doorways to a single authentication event. SecureLogin handles everything else. Your users will love you when you solve this problem for them.

Novell remains one of the pre-eminent providers of network security in the world. SecureLogin 3.5 continues that tradition of excellence with a single sign-on solution that provides everything you need: flexibility to work with your existing infrastructure; exceptional performance and scalability; and a comprehensive solution that addresses not only single sign-on, but additional concerns that are critical to keep workstations secure in today's mobile world.

So let your users define all the digital doorways they need on the Net. SecureLogin will manage it, secure it, and strengthen it. You make the Net a better place to work and save your organization a pretty penny in the process.

Feels good to be a hero, doesn't it? **N**

www.
caminosoft
.com