

# Rethinking SECURITY

## Seven Steps To Tighten Network Security

by Alan Mark

Since the events of September 11, 2001, people everywhere have been evaluating what security means to them. Many people are afraid to fly because they think it is too risky. After all, if you are a frequent flier, you know the challenges that officials face when trying to secure an airport.

Other people have avoided visiting major cities because of possible terrorism. Some people have been reluctant to attend sporting events such as the World Series. These are expected reactions for the general public.

In the IT world, we too have been rethinking how security affects our lives. On September 24, the *New York Times* reported that the terrorist attacks also “destroyed crucial links to state computers that manage welfare, Medicaid and food stamp cases, leaving thousands of poor people in New York City and nearby counties without normal access to emergency cash, food and health care.” (See Nina Bernstein, “Destroyed Computer Links Leave Thousands of Poor People Without Welfare Benefits,” *New York Times*, Sept. 24, at [www.nytimes.com](http://www.nytimes.com).) Clearly, the information highway is just as important as the buildings that house the records.

Security has always been an integral part of the IT infrastructure, and like airport officials, we face enormous challenges in securing our company’s networks. Security threats can be both electronic and physical. Electronic threats include hackers and intruders who attack web sites, e-mail systems, or in-house software. Physical threats include rogue network administrators, employees, and contractors as well as fires, bombs, floods, and earthquakes.

When a security breach is discovered, losses follow even if no damage is incurred. For example, if a security breach occurs in an airport, all passengers are evacuated, possibly causing delays in the whole air-transit system. If a company discovers an electronic break-in, that company may shut down its Internet access to prevent further intrusion. Of course, shutting down Internet access also stops electronic business transactions from customers, vendors, and remote offices. How can we as IT professionals minimize security violations and the resulting losses?

### RESPONDING TO THREATS

Our response to traumatic events is not always logical: For example, pocketknives, nail files, and other small devices are now banned on commercial flights. In fact, metal cutlery knives



have been banned from all airplanes and airports. Passengers receive a metal fork and a plastic knife with which to eat their meal (even at airport restaurants). Restricting a cutlery knife wouldn’t have prevented the tragedies on September 11, but any knife is now perceived as dangerous.

In the IT world, some software products have continual security vulnerabilities. For example, the Code Red worm, which exposed a security vulnerability in Microsoft Internet Information Servers (IIS), cost companies an estimated U.S. \$2.62 billion, according to researchers at Computer Economics. (See “Economic Impact of Malicious Code Attacks” at [www.computereconomics.com](http://www.computereconomics.com).) Although Netcraft estimates a slight drop in the usage of Microsoft IIS servers in the fall of 2001 (after the Code Red worm had hit), more than three million Microsoft IIS servers were still in use in November 2001. (Netcraft estimates there were 300,000 less Microsoft IIS servers in use in November than there were in October. For more information, see [www.netcraft.com](http://www.netcraft.com).)

The level of risk we take in all areas of life depends on what the perceived threats are and how we can respond to those threats and recover from any subsequent damage. Clearly, we must reevaluate security that seemed acceptable before September 11. We have entered an era where simple passwords and tape backup systems don’t provide adequate security. Now more than ever, we must design computer systems that minimize security risks and create plans that can be activated if a disaster strikes.

When setting up or evaluating security, security professionals adhere to three important principles:

1. Security is only as good as the weakest link in a chain of systems. You must implement strong security policies for an entire system. Otherwise, security policies are pointless.
2. Security is never 100 percent. In the real world, you cannot secure everything. However, you must continue to implement

**Please visit our advertiser  
ACCPAC International Inc.  
at [www.faxserve.com](http://www.faxserve.com).**

## Checklist for Evaluating Your IT Infrastructure

1. Maintain a current network architecture diagram, and use this diagram to determine where and how outside intruders can enter the network. Test your company's systems with hacker tools to identify security vulnerabilities, or hire an outside consultant to test them for you.
2. Create a list of all mission-critical servers and systems, their installation date, installer, and patches. Visit security-related web sites for the latest threats and the patches to fix them.
3. Create a list of policies for all network administrators to follow. The first (and most important) policy should be ensuring that you install the latest patches for the software you are running. Other policies should include subscribing to vendor mailing lists and frequently changing passwords on key systems (or using tokens or smart cards). You should also determine who is responsible for each system and the data that reside on it.
4. Create an employee policy that explains the appropriate use of information systems. For example, you should list the steps users take if they suspect a workstation is infected with a virus. You should also outline your company's policy on users trading passwords with each other, leaving desktops unattended, and keeping confidential data secure.
5. Evaluate how data are stored and accessed. Is your e-mail system secure? Is confidential data stored on local hard drives (especially laptops) without being backed up to network servers? Are data encrypted over the wire? If data are encrypted on a storage device, can that data be recovered if an employee leaves or is incapacitated? What if a laptop is stolen or dropped? Can data be recovered?
6. Determine the impact if you must disconnect systems from the Internet because of hackers.
7. Determine the impact if a fire or other disaster occurs in your company's data center. Do you have alternative venues to set up shop?
8. Determine the impact if you lose a key person due to death or illness.
9. Set up electronic auditing to monitor all activity on your company's directory and servers. Products such as Visual Click's DSMeter and DSRazor ([www.visualclick.com](http://www.visualclick.com)) and NetVision's DirectoryAlert ([www.netvision.com](http://www.netvision.com)) allow you to generate detailed reports on users and network events. Adrem Software's NetTrend ([www.adremsoft.com](http://www.adremsoft.com)) also monitors many network events.
10. Are network administrators paid well? Consider the U.S. airport screeners who are paid minimum wage. These people are responsible for traveling safety in the United States, yet get paid less than a fast food employee. Just raising their salaries won't increase their performance, but this action will encourage better candidates to apply for jobs. The same is true for network administrators. (For more information about the importance of the human element, visit [www.humanfirewall.org](http://www.humanfirewall.org).) ●

and test new procedures to attain the highest level of security possible.

3. Someone must be trusted. For example, having military personnel with machine guns guard airport-screening areas is only effective if the military personnel have gone through rigorous background checks. In the IT world, network administrators must be trusted to maintain systems, to control access to data, and to protect the internal workings of the IT infrastructure.

How do you ensure that network administrators can be trusted? You can create a circle of trust and human redundancy, whereby a group of network administrators is responsible for maintaining systems and these administrators periodically cross-train one another. You should also have network administrators periodically rotate tasks. In this way, if one network administrator does something out of the ordinary, another administrator will probably discover and report the violation.

No one is immune to sabotage and disasters. Even before September 11, the White House was the victim of a denial-of-service attack with the Code Red

worm. Ask yourself a difficult question: If you can't fully secure your company's network all at once, what steps should you take to begin the process?

This article explores the first steps you should take to tighten security on your company's network and to minimize security vulnerabilities.

### STEP 1: EVALUATE YOUR COMPANY'S ENVIRONMENT

The phrase, "if it ain't broken, don't fix it" doesn't apply to the IT world. If you followed this principle, you would never apply security patches or install virus software as long as users could still access their applications. Obviously, you cannot ignore network security until that security is compromised.

The most difficult aspect of implementing security is defining it. The basis of any security program involves three principles: integrity, confidentiality, and availability. In other words, a security program should 1) prevent data from being maliciously manipulated, 2) allow data to be seen by a select group, and 3) make data accessible to only those who need that data.

Several companies specialize in full-service security audits (also known as

vulnerability or risk assessments). These Managed Security Service Providers (MSSPs) can evaluate nearly every aspect of your organization's IT environment, including identifying who can physically access critical data systems. (For fun, you may want to rent the movie "Sneakers" to see how Robert Redford's company evaluated a bank's security system.) The cost for this service can range from tens of thousands of dollars to hundreds of thousands of dollars, and the evaluation can take several months to perform.

Is such an audit worth the money and effort? As in your personal life, you must assess what your company's assets are worth. Of course, you must factor in items that have no calculable value, such as photos or other items that cannot be replaced. For example, if you bought a home for U.S. \$150,000, you would purchase that much insurance for it. If your deductible were U.S. \$500, adding a U.S. \$300 alarm system would make sense. More importantly, the alarm would protect uninsurable items.

How do you evaluate how much your company's data are really worth? Unfortunately, it's difficult. Imagine if you suddenly lost your e-mail address book. How

Please visit our advertiser NetVision at  
[www.netvision.com](http://www.netvision.com).



**Figure 1.** Fingerprint readers are a reliable and secure authentication method. NMAS enables you to add such biometric authentication methods to your existing network.

long would you spend recreating the list? Or what would happen if your company's sales database system were infected by a virus? If the backup took one day to restore (not unreasonable given the size of today's databases), how much revenue would your company lose?

You also can't easily compute a return on investment (ROI) from implementing most security solutions, except those solutions that add functionality to an existing system. For example, if a home alarm included a camera to check your premises via the Internet, that alarm would serve a double benefit. In the business world, where reducing support calls results in cost savings, you may have an easier time selling a single sign-on solution to upper management.

You can't put a dollar figure on vulnerability because it's merely a threat. Are there still safe towns where people don't lock their doors at night? In the Internet age, your company's doors are always open, and the entire world is just outside.

Although you can't easily determine how much your company's data are worth, you can determine what would happen if your company's data suddenly disappeared. In your evaluation, consider a worst-case scenario (such as a fire and complete destruction) and a more likely scenario (such as sabotage by intruders and hackers).

Depending on your company's business, another area of concern may exist: industrial espionage. Although a typical hacker (also known as a *cracker* or *script kiddie*) wants to be seen and heard, an industrial intruder's goal is to steal information without detection. The industry

does not have hard evidence on how much spying occurs because many thefts go unnoticed.

Evaluating your company's environment can be an overwhelming task. The best approach is a step-by-step analysis, beginning with a current diagram of your company's network architecture. The "Checklist for Evaluating Your IT Infrastructure" will help you evaluate entry points and critical

processes on your company's network. (See p. 8.) This checklist will also help you address security issues such as determining how confidential data is accessed and who can access it.

Perhaps the most overlooked part of a security analysis is writing policies. For example, you should write policies to ensure that software patches are installed, only authorized users can enter the data center, and smart cards are required to use the accounting system.

In fact, ensuring that software patches are installed is critical. I am amazed to read about companies that connect unpatched systems to the Internet. Patches often fix security vulnerabilities. If you do not apply patches, your systems may have gaping security holes. Scanners find these vulnerable systems and alert hackers.

You should not connect any system to the Internet unless that system is fully patched. To ensure that the software on your company's network is completely up-to-date, you should maintain a good relationship with your vendors and review service level agreements (SLAs) with them.

Policies are both electronic and written. You can use ZENworks for Desktops or a similar product to enforce electronic policies, such as users can access only certain applications from certain workstations. You must write policies to inform employees that they should not share passwords or use another person's workstation without first authenticating to the network or to the workstation. (For more information about implementing security policies, read "Generally Accepted System Security Principles" at <http://web.mit.edu/security/www/gassp1.html>.)

As we learned from the disasters of September 11, police and militia alone



**Figure 2.** Some biometric devices use face or eye recognition to authenticate users to the network. Again, NMAS supports such devices, allowing you to implement this added protection on your company's existing network.

Please visit our advertiser Saflink at  
[www.saflink.com](http://www.saflink.com).

## Novell Access and Security Solutions

Controlling access to network resources is critical to establishing and maintaining security on your company's network. Because your company's network includes multiple operating systems and mission-critical applications that require separate authentication, controlling access to all of these systems can be a complicated and time-consuming task.

Novell access and security solutions help you eliminate the boundaries between platforms and applications, allowing you to more easily manage users and network resources. In addition, these solutions also better protect network resources and confidential information, and help users access the applications and information they need more easily.

- **Novell eDirectory** ([www.novell.com/products/nds](http://www.novell.com/products/nds)). eDirectory is a cross-platform Lightweight Directory Access Protocol (LDAP)-compliant directory that provides a central repository for identity information, authentication credentials (such as fingerprints), and access control policies. Not surprisingly, eDirectory is the foundation for Novell access and security solutions.
- **Novell Account Management** ([www.novell.com/products/nds/accountmanagement](http://www.novell.com/products/nds/accountmanagement)). This eDirectory-enabled application simplifies and unifies the management of user profiles on Windows 2000, Windows NT, Solaris, and Linux servers. Rather than managing separate accounts on each platform, you can simply manage one account in eDirectory. Users then have only one set of credentials they can use to access all of the network resources to which they have rights.
- **NDS Authentication Services** ([http://developer.novell.com/nss\\_profile.jsp?product\\_key=79958](http://developer.novell.com/nss_profile.jsp?product_key=79958)). NDS Authentication Services enables you to easily manage access to different platforms on your network by extending NDS authentication services to non-NetWare operating systems. With NDS Authentication Services, you can synchronize user account information on NetWare, Windows 2000, Windows NT, Solaris, Linux, OS/390, and UNIX platforms. To synchronize this information, you create policies and business rules that are stored in eDirectory.
- **Novell Modular Authentication Service (NMAS) Enterprise Edition** ([www.novell.com/products/nmas](http://www.novell.com/products/nmas)). NMAS enables you

to better protect network resources through multifactor authentication mechanisms. With NMAS, you can deploy any combination of authentication methods including passwords, smart cards, tokens, biometrics, proximity cards, and digital certificates.

NMAS also protects NetWare volumes through graded authentication, which tightens security through a combination of grades, security labels, and clearance levels. Graded authentication better protects resources by requiring users to log in using a login sequence that matches their security clearance, which, in turn, must match the grade of the resource users want to access.

- **Novell SecureLogin** ([www.novell.com/products/securelogin](http://www.novell.com/products/securelogin)). Novell SecureLogin provides single sign-on services to hosts, mainframes, web sites, Citrix sessions, and Windows applications. Novell SecureLogin also includes password rules, directory-based sign-on applications, and support for NMAS.
- **Novell iChain** ([www.novell.com/products/ichain](http://www.novell.com/products/ichain)). Novell iChain enables you to secure access to web applications and resources. iChain supports multifactor authentication and secures access to web applications and resources without requiring you to install an agent on each protected web server.
- **Novell BorderManager Enterprise Edition** ([www.novell.com/products/bordermanager](http://www.novell.com/products/bordermanager)). BorderManager enables you to integrate protection against internal and external threats, control access to Internet sites, and manage remote user access to company data. Like iChain, BorderManager includes proxy cache services.

To see how companies are using these solutions to tighten their network security, see "Taipei County Government Secures Access to Its Assets" (see p. 24) and "Beneficial Life Opens Its Internet Doors to Clients, Agents, and Employees" (see p. 36). (For more information about these solutions, you can attend a web seminar hosted by Novell. See "Novell Web Seminar: Hear All About It" on p. 20.)

To help customers control access to their organization's networks, Novell will soon release an integrated solution that includes all of the features and capabilities now available in the Novell access and security solutions. (Look for more information about this integrated solution in upcoming issues of *Novell Connection*, or watch for information on Novell's web site at [www.novell.com](http://www.novell.com).) ●

cannot secure the world. Everyone must be involved and alert. You should explain to employees how important it is for them to speak up if something does not seem right or if they discover a security flaw. You may even want to set up an anonymous mailbox for users to write suggestions or send information about security issues.

You should also warn users about the danger of e-mail messages. Just as the U.S. Post Office advises people not to open letters from unknown senders, you should advise users not to open e-mail messages from unknown senders—especially e-mail messages that have

attachments. Because the temptation to open these messages can be too great for some users, you may want to filter suspicious e-mail messages at the gateway before they reach users.

Another important system to implement is electronic auditing. Some excellent products monitor both NetWare and eDirectory: Visual Click's DSMeter and DSRazor ([www.visualclick.com](http://www.visualclick.com)), Blue Lance's LT Auditor+ ([www.bluelance.com](http://www.bluelance.com)), and NetVision's DirectoryAlert ([www.netvision.com](http://www.netvision.com)). In addition, AdRem Software's NetTrend ([www.adremsoft.com](http://www.adremsoft.com)) monitors many network devices.

These products generate detailed reports about nearly any activity that occurs in eDirectory or on a server. For example, using one of these products, you can see which users have administrator rights and if these users' rights are hidden through access control lists (ACLs). You can also generate reports on password settings and failed logins to eDirectory.

In particular, DSMeter logs eDirectory and NetWare file system security changes, and DSRazor audits eDirectory security and includes more than 100 predefined reports. DirectoryAlert and LT Auditor+ feature real-time intruder alerts and secure audit trails. Implementing one of these

systems is crucial to knowing what is happening on your company's network.

## STEP 2: IDENTIFY YOUR USERS

The basic part of any computer system is identifying the user. The main problem is that each system implements a different procedure to identify a user. As a result, user BOB in one system may be different than user BOB in another system.

For years, companies have explored consolidating user accounts, without much success. Unfortunately, most systems do not communicate with each other, and companies may not be able to replace legacy systems with newer standards-based applications. So what's a poor network administrator to do?

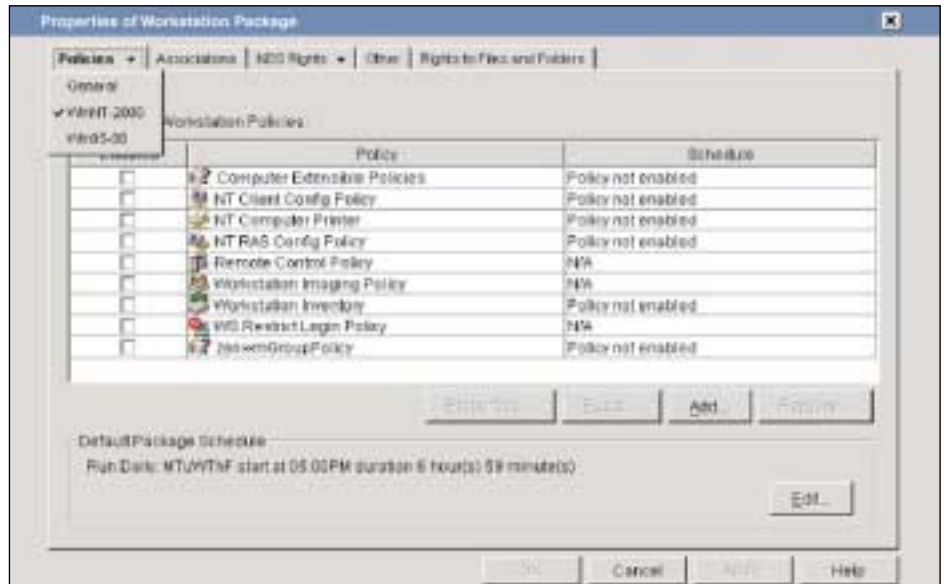
For starters, you may want to try Novell access and security solutions, which coordinate the tedious task of creating, deleting, and identifying users. Novell access and security solutions enable organizations to securely manage access to applications, databases, and platforms for web, wireless, client, Virtual Private Network (VPN), and dial-up users. With these platform-independent solutions, users have only one set of credentials to access all of the network resources to which they have rights. And, of course, it doesn't matter which platform these resources run on. (For a list of these solutions, see "Novell Access and Security Solutions.")

The identification process in any system ranges from a simple username and password to complex biometric IDs. Remember the secure lab in the first "Mission Impossible" movie? In that movie, the U.S. CIA used a variety of sensors, biometric, and smart card techniques to protect a super-sensitive system.

In the real world, of course, most companies can't afford such fancy techniques. However, relying on only a password to protect critical information isn't adequate anymore. Fortunately, you can improve the methods you use to identify users.

Identifying a user can include three basic login factors: password (something you know), token (something you have), and biometrics (something you are). Combining these factors results in a *multifactor authentication*, which essentially proves a user's identity. A *clearance level* (also called a *grade*) is assigned to the user, and data are restricted based on this clearance level.

For example, you could set up a system so that a user who authenticates with a



**Figure 3.** Novell's ZENworks for Desktops allows you to create workstation policies, which you can use to tighten security. For example, you force regular virus scans and backups of workstations.

username and password can access only basic applications and data. If a user authenticates with a fingerprint, however, that user can access more sensitive information such as the payroll system.

Novell Modular Authentication Service (NMAS) Enterprise Edition uses Novell and third-party modules to implement any or all of these login methods. (NMAS is a Novell access and security solution. For more information about NMAS modules, visit [www.novell.com/products/nmas/partners](http://www.novell.com/products/nmas/partners).) The login methods you choose depend on how much trust you require to access a resource, the cost of implementing the method, and whether or not the method is used for other functions. You can choose from the following options:

- **Password.** The NDS password has been the basis of authentication since 1993. Two other password options are available: the simple password and the enhanced password.

The simple password stores another encrypted phrase in eDirectory and is used by various Novell products (such as Native File Access Pack). The simple password can also be used for Internet-related functions. The NDS password, on the other hand, is never sent across the wire and is inaccessible to applications. (For more information, visit <http://developer.novell.com/research/appnotes/1994/october/02/04.htm>.) The

enhanced password allows you to set up rules for the password (such as passwords must include upper- or lowercase letters, numbers, or special characters).

In addition, a Personal Identification Number (PIN) can be used to unlock smart cards or can be combined with token devices to identify a user.

Passwords are well-suited for web-based authentication because no special hardware is required. However, passwords are more easily stolen and hacked than other methods, and they can be written down.

- **Token.** Most tokens are double-factor based: They require something that you know (password or PIN) and something that you have (the device). Some smart card readers also have a fingerprint reader for added protection (biometric). (See Figure 1 on p. 10.)

Several types of tokens are available today. The most popular is SecureID from RSA Security Inc. ([www.rsasecurity.com](http://www.rsasecurity.com)). This time synchronous token displays a new six-digit code every 30 seconds. The user enters the code plus a PIN to authenticate.

In a similar fashion, Vasco ([www.vasco.com](http://www.vasco.com)) offers Digipass, a token that displays a six-digit number but only after the user enters the correct PIN. The device offers a challenge-response option that doesn't require a precise clock in the server. Like SecureID, Digipass is well-suited for Internet or intranet use.

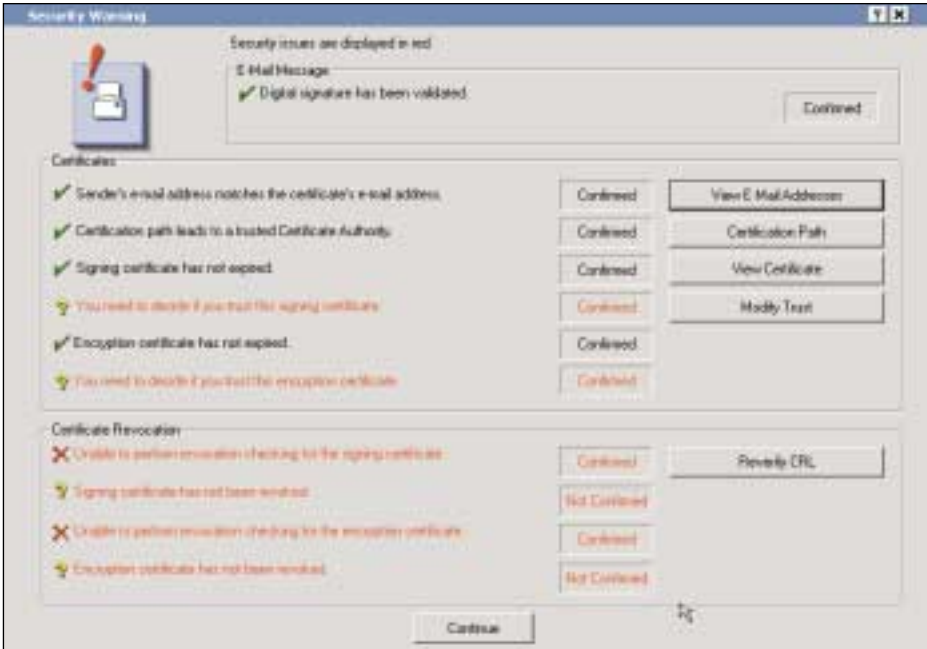


Figure 4. GroupWise 6 helps users implement digital certificates, which verify the identity of the sender and protect the integrity of the message.

Rainbow Technologies Inc. ([www.rainbow.com](http://www.rainbow.com)) offers a small USB token that stores users' credentials and certificates. A password unlocks the token for use. Because the USB token requires special software to be installed on the PC, this token won't work at Internet cafes.

Most smart cards operate in a similar fashion. The user puts the smart card into the reader, unlocks the smart card with a PIN, and the credentials are used to authenticate the user.

Smart cards and USB tokens have two advantages over other devices: The workstation can be locked when the device is removed, and a private key stored on the device can be used to digitally sign a transaction (such as an e-mail message).

A new device, called a *proximity card*, is also available. A sensor is attached to a workstation, and this sensor automatically recognizes the card the user is carrying as he or she approaches. To prevent a thief from automatically authenticating with a stolen card, an additional form of ID is required (usually fingerprint). This solution is being implemented in some hospitals for fast terminal access.

- **Biometric.** How does the non-computing world identify a person? By the way he or she looks. In small organizations, people easily recognize their colleagues.

In larger organizations or in public, however, people rely on ID cards.

ID cards have three problems: First, people's appearances (such as hair color, beards, wrinkles) change over time so ID cards must be updated. Second, ID cards may be easy to forge. Third, photo ID cards don't translate well in the electronic world.

Obviously, we need a different approach for network IDs. Biometric techniques have been around for a while, but until recently, they weren't reliable. Today, biometric devices can accurately identify a user by his or her fingerprint. (See Figure 1 on p. 10.) Other methods, such as voice and face recognition, are also possible. (See Figure 2 on p. 10.) SAFLINK Corp. ([www.saflink.com](http://www.saflink.com)) supports a variety of biometric devices ([www.saflink.com/bsp.html](http://www.saflink.com/bsp.html)) and uses NMAS as the authentication platform.

Of course, the trick is that the biometric reader cannot produce false positives. In other words, the reader cannot mistakenly identify you as someone else and authenticate you with the wrong ID.

TLC Care Hospital in Las Vegas uses a hand-geometry device to authenticate employees when they start and stop work. This system ensures that no one can punch in or out for another person. In addition, 55,000 employees at Chicago airports will soon use finger-

print identification to access secure areas. This fingerprint identification will be provided by SecuGen, another NMAS partner.

### STEP 3: EFFICIENTLY MANAGE USER ACCOUNTS

Most users have multiple user accounts. For example, suppose that Alice has an Alice Windows account on her workstation and logs in to eDirectory as Alice. However, Alice's e-mail ID is AliceW, and when Alice accesses a UNIX-based payroll application, she's known as AliceWinters. Alice's mainframe ID is AW09379 (her initials and employee ID). Of course, each account has a different password. What's Alice to do?

You know only too well that multiple accounts cause headaches for you and the users' whose accounts you manage. Lost passwords mean more telephone calls to the help desk, resulting in U.S. \$50-\$80 per incident according to IDC. (For more information, visit [www.idc.com](http://www.idc.com).) And what happens if "Alice doesn't live here anymore?" How quickly can you disable all of her accounts?

Old systems may fade away, but they never die because they're too costly to change. So you're stuck trying to teach new tricks to old systems. Fortunately, several solutions can help you manage user identities on multiple platforms.

The first solution is NDS Authentication Services ([http://developer.novell.com/nss\\_profile.jsp?product\\_key=79958](http://developer.novell.com/nss_profile.jsp?product_key=79958)). This solution synchronizes passwords between the following systems, even if the usernames are different:

- AIX
- FreeBSD
- HP-UX
- Linux
- OS/390
- Solaris
- Windows NT/2000

With NDS Authentication Services, Alice uses the same password—her eDirectory password—to access her applications, regardless of the platform on which the applications are running. Some applications can also access eDirectory user properties, such as group membership and security equivalence.

Another solution, Novell DirXML ([www.novell.com/products/nds/dirxml](http://www.novell.com/products/nds/dirxml)), synchronizes not only usernames and

Please visit our advertiser TestOut at  
[www.testout.com](http://www.testout.com).

**Please visit our advertiser Novell Inc. at  
[www.novell.com](http://www.novell.com).**

**Please visit our advertiser Novell Inc. at  
[www.novell.com](http://www.novell.com).**

passwords but also other user-related data. For example, when a user's address and phone number are changed in an Oracle database, Novell DirXML can send that change to eDirectory and other databases and programs such as your company's e-mail system. As a result, the change is made only one time, and all of your company's databases and addresses books contain current information.

In fact, eDirectory and DirXML are the foundation of Novell's Zero Day Start initiative. This eProvisioning solution sets the standard for synchronizing disparate systems in an organization. With Zero Day Start, new Novell employees can be productive the first day they start work. Rather than entering employees' information in multiple systems (a process that could take days or even weeks), Novell can enter this information only once. The information is then synchronized with the appropriate systems.

Equally important, this solution makes Zero Day Stop a reality. You know that quickly removing or disabling user accounts can be a nightmare. With Novell DirXML, you can disable user accounts with the click of a button.

In addition, NetVision's Synchronicity ([www.netvision.com](http://www.netvision.com)) manages multiple Windows NT domains by using eDirectory as the synchronizing mechanism and single point of reference. NetVision also recently announced NetVision Policy Management Suite, which automates the process of synchronizing passwords on disparate systems. This suite includes a library of scripts that help enforce security policies on those systems.

**STEP 4: PROTECT PASSWORDS**

Face it: most systems—UNIX systems, mainframes, and web sites—use passwords as their only method of authentication. Despite all that's been said about tokens, smart cards, and biometrics, the unforgiving weak password is probably still your worst nightmare.

Where do users keep their list of passwords? This list may be written on a sticky note and placed under a keyboard or on a monitor. It may even be stored on a laptop or hand-held device. If a simple solution to the password chaos isn't available, users will creatively devise methods of their own—even at the risk of having their passwords stolen.

The answer to this password dilemma is Novell SecureLogin, which protects your organization from the plethora of problems related to the unsophisticated collection of characters known as the password. First, Novell SecureLogin provides single sign-on services to web, host, Citrix sessions, and Windows applications. Second, Novell SecureLogin incorporates directory-based password policies, which you create. Finally, because the user's credentials are stored in the directory, they are accessible from any workstation that is running the Novell SecureLogin software.

With Novell SecureLogin, dozens of applications are predefined for automatic password detection. In this case, Novell SecureLogin automatically stores and

*Storing data locally presents two problems: Data probably won't be backed up, and data is easily accessible if the workstation is stolen or hacked.*

remembers the user's credentials with minimal user interaction.

If the application is not predefined, Novell SecureLogin includes a wizard to help the user set up a single sign-on application. For web-based logins, Novell SecureLogin asks the user whether or not it should remember the user's credentials (username, password, and other data).

The traditional concern over single sign-on services has been that one password unlocks all other passwords. If the eDirectory password is stolen or hacked, someone may be able to access a mission-critical application because the username and password are automatically entered. To prevent this problem, you can use NMAS to require stronger eDirectory authentication. Before Novell SecureLogin enters the user's credentials for the mission-critical application, another form of ID must be verified (such as a token or fingerprint).

What if the user authenticates to eDirectory and leaves to get a cup of coffee? The workstation is now open to any passer-by. At least two solutions are

available: You can configure NMAS to lock the workstation after so many minutes of inactivity, or you can use a smart card or token to secure the workstation. If this smart card or token is removed, the workstation is automatically locked.

This last alternative requires the employee to take the token when leaving the workstation. Attaching the token to a key chain or photo ID card helps ensure employee compliance.

I speak to thousands of network administrators every year on various security topics, and I am amazed that many don't use a single sign-on product. Such a product not only increases password security but also saves you time. Try it out; download a demo version of Novell SecureLogin from [www.novell.com/products/securelogin](http://www.novell.com/products/securelogin), and use it on your own workstation in standalone mode. On my own workstation, I have defined more than 50 credentials to applications and web sites.

**STEP 5: SECURE WORKSTATIONS AND SERVER CONSOLES**

Today's workstations store more data than servers did five years ago, and therein lies the problem: When storage is readily available on drive C, users have no reason to save data elsewhere.

Storing data locally presents two problems: Data probably won't be backed up, and data is easily accessible if the workstation is stolen or hacked.

Novell's ZENworks for Desktops ([www.novell.com/products/zenworks](http://www.novell.com/products/zenworks)) uses eDirectory to enforce workstation policies. (See Figure 3 on p. 13.) With ZENworks for Desktops, users and workstations become manageable entities and are associated with inheritable policies. For example, you can create a policy that forces a virus scan and backup of a workstation—whether or not the user is logged in to the network. With Wake-Up On LAN technology, a PC can be powered on via remote commands.

In addition, ZENworks for Desktops policies can dynamically create eDirectory users on Windows workstations. A user's profile is then copied from the user's home directory to the workstation, and another policy dictates what the user can see and do.

For example, after Alice authenticates to eDirectory, her desktop environment and preferences are created on the workstation. A ZENworks for Desktops policy

prohibits Alice from accessing the Explorer, Run, and Registry commands, thereby preventing her from accessing external applications. When Alice logs out, her profile is updated on the server and removed from the workstation, preventing anyone else from accessing Alice's account.

The key to ZENworks for Desktops is eDirectory, which is the keeper of user and workstation information and the policies that affect them. If Alice's eDirectory account is disabled, she won't be able to log in to any workstation.

ZENworks for Desktops also includes the Application Launcher, which installs, distributes, launches, configures, repairs, and uninstalls nearly any Windows application. The most important security feature of Application Launcher is that if a user doesn't have rights to the application, that user can't even see the icon to double-click it. Hackers have a difficult time breaking into systems they can't see.

Of course, you should also secure the server console. The traditional RCONSOLE utility is considered unsafe to use because passwords aren't securely en-

rypted. To solve this problem, AdRem's sfConsole 4.0 provides secure access to both local and remote server consoles. With sfConsole, you simply authenticate to eDirectory and establish a secure 128-bit key connection.

In addition, sfConsole 4.0 safeguards the server console with a password-protected screensaver and keyboard blockade. You can also grant certain users limited rights to the server console, and you can specify which commands these users can execute at the server console.

#### **STEP 6: SECURE DATA**

Securing data is a complicated undertaking. After all, data has to be usable, which means it can be printed or viewed on a monitor. With networks, information is also easily copied, and if everyone has access to the network, an eavesdropper can capture data sent across the wire.

You can take two approaches to securing data: You can prevent unauthorized people from accessing data, and you can encrypt data in case an unauthorized person gains access to it.

In the NetWare environment, you can place access control on volumes, directories, and files. In eDirectory, you can restrict which objects or attributes can be seen or modified. However, if an intruder steals a password—or maybe even a server—data are exposed. You must encrypt data over network wires and on the hard drive itself.

As mentioned earlier, NMAS can add a security label to a NetWare volume, requiring all users—even the ADMIN user—to authenticate a certain way before they can view data stored on the volume. For example, if the FINANCE volume has a Password&Token label, a user would need at least that clearance level to see stock information. This clearance level means the user would need to use a token such as a smart card and PIN. With NMAS, how users authenticate determines what they can do. (For more information about using clearance levels, see "Taipei County Government Secures Access to Its Assets" on p. 24.)

Novell iFolder ([www.novell.com/products/ifolder](http://www.novell.com/products/ifolder)) safely synchronizes data

**Please visit our advertiser Printer Properties Pro at  
[www.PrinterPropertiesPro.com](http://www.PrinterPropertiesPro.com).**

## Novell Web Seminar: Hear All About It

If you would like more information about Novell access and security solutions, you may want to attend the Novell Access and Security web seminar. Held twice a day on January 29, 30, and 31, the Novell Access and Security web seminar will cover security topics such as the following:

- Using graded authentication to tighten security
- Controlling access to network re-

sources, such as enabling partners, suppliers, or customers to access specific information

- Eliminating the hassle of managing multiple accounts and multiple passwords for those accounts

Every person who "attends" the web seminar is registered to win a biometric fingerprint reader from SAFLINK Corp. To register, visit [www.novellsecurity.com](http://www.novellsecurity.com) or call 1-800-274-6404. Only a limited number of people can attend the web seminar, so you may want to register early. ●

between workstations and servers. Files stored in a specified folder are encrypted before being sent to the server. Even if someone were to steal the server, the encrypted data are worthless to the thief. However, users with the necessary rights can securely access files from any web browser. iFolder uses Secure Sockets Layer (SSL) to protect the transmission. (For more information, see "Novell iFolder: Your Data Where You Want It, When You Want It," *Novell Connection*, May 2001, pp. 6-20. You can download this article from [www.ncmag.com/past](http://www.ncmag.com/past).)

Encrypting data is an effective way to thwart thieves. But how do you know that the data hasn't been tampered with? Encryption keeps the data safe; digital signatures help ensure data integrity.

When an e-mail message or file is digitally signed, the recipient can be sure that it came from the sender and wasn't tampered with. The biggest problem with encrypting or signing a document is getting the credentials (public keys) of the sender and recipient. The details of digital signatures are beyond the scope of this article, but in general, in order for Alice to send an encrypted message to Bob, she needs Bob's public key. In order for Bob to verify that the message came from Alice, he needs Alice's public key.

GroupWise 6 includes new features that help solve the problem of finding a user's public keys. Before Alice sends her message, GroupWise prompts her to use a private or public LDAP directory to find Bob's key. Once found, the certificate (including Bob's public key) is stored in Alice's address book. (See Figure 4 on p. 14.)

If you are looking for software to secure e-mail messages, PGP Security Business, a

division of Network Associates, encrypts and signs files and e-mail on multiple platforms. A huge database of users freely uses the software. (For more information about PGP products, visit [www.pgp.com](http://www.pgp.com).)

A new approach to data encryption is to require two or more authentication factors to encrypt files, folders, or an entire hard drive. After the user authenticates to the local system, the user's passphrase is sent to the encryption software. PC Guardian ([www.pcgardian.com](http://www.pcgardian.com)) has several products on the market to protect data, and this company is developing a version that works with eDirectory.

Although laptops make working on the road easier than ever, they are the least secure piece of equipment an organization owns. Hundreds of thousands of laptops are stolen each year (1 in 14 of all manufactured), and I'll bet that most of the data are unprotected. (For more information, visit [www.ztrace.com/zLab1.asp](http://www.ztrace.com/zLab1.asp). For statistics on lost computers, visit [www.safeware.com/losscharts.htm](http://www.safeware.com/losscharts.htm).)

Even if the laptop operating system requires a password, a hacker with the right tools can eventually break it. If the laptop isn't backed up, data are lost with the hardware. Using ZENworks for Desktops to set up workstation policies that require laptops to be backed up and using Novell iFolder to synchronize data between workstations and servers can make laptops much more secure.

As you know only too well, viruses, worms and other nasty creatures can infect workstations and possibly make them unusable. Worse yet, viruses and worms can send sensitive data to a host on the Internet. Viruses infect systems in three basic ways: through a security hole in client software (such as Microsoft Windows,

Outlook, or Word), by gaining access to web services (through Microsoft IIS or a UNIX-based application), or via e-mail.

Again, you can use ZENworks for Desktops to force regular virus scans, and your security policy can explain why users should not open e-mail messages or attachments from unknown senders. You may also want to scan e-mail messages at the gateway.

### STEPS 7: SECURE INTERNET ACCESS

Managing internal users and systems can be difficult, but when users need to access internal systems via the Internet, you probably get justifiably nervous. And when vendors and customers also need access, you may feel like opening your medicine cabinet before proceeding.

Your first line of defense is the so-called *firewall*. Yes, that one system will do everything from preventing disasters to keeping the bad guys out. It's a floor shine and a shoe polish!

I'm sorry to be so sarcastic, but *firewall* is the most misused word in the networking world. No one device can protect an entire network, nor should you rely on one device to do this. You should think of a firewall as a collection of systems, services, and policies that protect your internal network from intruders and data loss.

A *firewall solution*, therefore, encompasses software and hardware found on servers, Internet gateways, and even workstations. A complete firewall solution should include intruder-detection systems, authentication controls, auditing monitors, access management to hardware and data centers, virus software, and policies to enforce employees' compliance.

Before opening your network's floodgates to the outside world, you must determine which systems must be accessible. You will probably discover that nearly all of your company's systems must be accessible to Internet users. Because many systems are now or will be web-based, you need to identify users via a web browser interface.

Novell's iChain puts a front-end on corporate resources by requiring users to authenticate by password, token, or certificate before those users access back-end systems. In addition, HTTP data is automatically encrypted within an SSL session established by iChain. As a result, all communications between the Internet user and the back-end web server are encrypted without changing the web server.

BorderManager provides another type of secure transaction with a VPN. Using VPNs, each client establishes a secure connection to a server. After authentication, users access the intranet as if they were in the office. Server-to-server VPNs encrypt data between servers using the Internet as the transport medium.

Data must be secured at all points. Although securing Internet transactions is important, protecting the back-end systems is imperative. There has not been one proven case of a credit card number being stolen in a single transaction. However, there have been many reports of intruders entering databases that contain credit card numbers. Both iChain and BorderManager can effectively block access to back-end systems.

#### **PUTTING IT TOGETHER, BIT BY BIT**

With eDirectory as the foundation of your company's network, you know who a user is (identity), where that user is (location), how that user logged in (authentication), and what that user can see (access control): The following real-life scenario shows the power of using eDirectory with other solutions mentioned in this article.

Bob arrives at his desk and logs in to eDirectory. His account is valid, so his profile is transferred to his workstation. It's Monday morning, and a new virus was discovered over the weekend. The ZENworks Application Launcher configures Bob's Start menu and taskbar, downloads the latest virus signature file, and begins running a virus check. Because Bob is in the Sales division, a ZENworks policy allows nearly full access to his workstation (although he cannot use Regedit).

Bob launches a terminal emulator to access a sales database. His mainframe ID is BobT. He enters his username and password (which was synchronized to his eDirectory password).

Bob next wants to check the financial system to see sales figures for his area. The financial system requires a biometric clearance, so Bob reauthenticates using a fingerprint reader on his keyboard. When the Application Launcher refreshes, the financial system icon appears on Bob's desktop.

Now Bob wants to check his stock holdings. He launches a browser and goes to the web site. Novell SecureLogin automatically enters his username and password for the web site. A free golfing lesson offer is shown in a pop-up window, and Bob clicks on it. However, he

can't access that web site. The network administrator used BorderManager to block sports-related sites.

Bob then launches GroupWise. Novell SecureLogin automatically enters his GroupWise username, but a dialog box appears, telling Bob that it's time to change his password. Novell SecureLogin automatically helps Bob create a new password based on rules defined by the network administrator.

Bob composes a message to his boss. Before sending the message, he encrypts and signs it. Now the message will be sent confidentially, and his boss can prove it came from Bob.

At home, Bob accesses the corporate intranet by first authenticating to the Novell iChain server. Thereafter, all communications between his home computer and the intranet are secured via SSL, and sign-on to corporate web applications are handled automatically.

#### **CONCLUSION**

Let's face it: security isn't sexy. Most security projects tighten the control over

users, workstations, and buildings. For that reason alone, cracking down on security worries some network administrators because they have to appear as bad guys.

Your organization will always be subject to security threats, both internal and external. Your job is to minimize the risk. Remember that security is an on-going process. Continually update your systems with the latest security patches, continually assess your environment for risks, and implement the best security systems your company can afford.

Finally, don't forget your most important resource: people. Users can be difficult, but they can also be your first line of defense. Ask them to be part of the security process. For example, while I was flying back from Comdex in November, a flight attendant asked me if I would be willing to help the crew if a bad situation occurred. In this new era of unexpected situations, everyone must be involved.

*Alan Mark is the chief security strategist for Novell. He has worked at the company for 11 years and speaks to large organizations around the globe. ●*

**Please visit our advertiser  
Biscom Inc.  
at [www.biscom.com](http://www.biscom.com).**