

SCANNING STUDENTS

A Stockholm School Goes Biometric

by Linda Kennard

in Stockholm, Sweden, children between the ages of six and 18 attend a course in computer literacy once or twice weekly as part of their compulsory education. (For more information about these computer courses, see “Stockholm Students Get Computer Savvy” on p. 8.) To thus enable students to become more familiar with computers, the IT Department for the City of Stockholm’s Executive Office equips each of the city’s approximately 150 public schools with one or two computer labs.

The IT Department stocks the schools’ labs with between 15 and 20 workstations and further endows many schools with two or more workstations per classroom. In each school, these workstations are connected to one another and to servers on the schools’ LANs. The schools’ LANs are in turn interconnected to form the Stockholm Schools Data Network. (For more information, see “Where the Pilot Runs” on p. 12.)

Until recently, all of Stockholm’s 85,000 students authenticated to the Stockholm Schools Data Network by entering their Novell eDirectory username and password at one of the network’s 25,000 workstations. (For more information about Stockholm, see “Did You Know . . .”) Stop right there and think for a moment about the frightening implications of that last sentence: 85,000 users—all under the age of 18—with passwords. As an administrator of adult network users, you can just imagine the types (and frequency) of problems that arise when you put passwords in the hands of children.

The good news is that the password problems in Stockholm’s schools may soon come to an end. In fact, the problems already have ended at Kvarnbysskolan, a primary school for children ages 6 through 12.

Since February 2001, Kvarnbysskolan in Rinkeby, one of Stockholm’s 18 boroughs (or counties), has been testing Novell Modular Authentication Service (NMAS) 1.0 (www.novell.com/products/



nmas) and SAFmodule for NMAS 2.0 from SAFLINK Corp. (www.saflink.com).

The Novell/SAFLINK solution replaces password authentication to eDirectory with biometric authentication or, in this case, fingerprint authentication. What this means to the 450 students and teachers enrolled in this pilot program is that they no longer have to remember and enter a password to log in to the Stockholm Schools Data Network. Instead, they get scanned—or at least their index fingers do.

Several benefits are inherent to the biometric authentication that this Novell/SAFLINK solution enables. For one thing, students can flaunt their fingertips wildly without any threat of compromising their accounts’ privacy or the network’s security. For another thing, students can’t authenticate using someone else’s fingertip. And last, but arguably most important, no matter how tired or scattered students are feeling, they never forget their fingertips.

In short, the Novell/SAFLINK solution that Kvarnbysskolan is using has done two things that are typically mutually exclusive: The solution has simultaneously increased both the convenience and security of network access. (See “Do You Care?” on p. 15.)

BIOMETRICS—SO YOU NEVER FORGET

Back up a moment: What does happen when you put passwords in the hands—or rather minds—of children? You won’t be the least bit surprised to learn that what happens is the same thing that happens when adults use passwords: You suffer the

Did You Know . . .

Built on 14 islands that are connected by bridges and canals, the city of Stockholm is sometimes called *Venice of the North*. Stockholm, the largest of Sweden’s 289 municipalities, celebrates its 750th anniversary this year.

Stockholm’s 736,000 residents are governed by a popularly elected city council that collects taxes and operates public services. For example, Stockholm’s 101-member city council manages its approximately 150 public primary and secondary schools. (Stockholm also has about 30 approved private schools.) For more information about Stockholm, visit www2.stockholm.se/english. ●

Visit our advertiser, ACCPAC at
www.faxserve.com.

Stockholm Students Get Computer Savvy

In Stockholm, Sweden, students start to gain computer know-how from the time they are six years old by attending mandatory computer literacy courses once or twice weekly. The length and content of these courses vary from school to school and also, as you probably would expect, depending on the age of the students.

For example, at Kvarnbysskolan, each homeroom class (to use American jargon) visits the computer lab twice weekly for courses that last up to 45 minutes. For the youngest students (ages six through 12), the courses are fairly rudimentary, designed primarily to help the students feel more comfortable using the computer. To that end, the courses for these young students concentrate on familiarizing them with the keyboard and mouse using applications designed for this purpose and for this particular age group.

Young students may also play alphabet and number games during their computer literacy course.

The computer literacy courses may also provide students of any age with the opportunity to watch educational streaming movies or listen to digitized radio programs. The media center on the Stockholm Schools Data Network stores more than 400 such streaming movies and roughly 1,400 digitized radio programs.

For older students, the computer literacy courses become more complex. For example, these older students learn how to install and manage Cisco, Novell, Linux, Sun, and Microsoft systems.

Ultimately, the simple point of these computer literacy courses is to teach students to “use the computer as a tool,” explains Samir Hamouni, project manager in the IT Department for the City of Stockholm’s Executive Office. ●

usual set of problems associated with password authentication.

For example, students frequently forget their password. Consequently, teachers find themselves spending the first several minutes of their 45-minute computer courses resetting passwords. To avoid the embarrassment of forgetting their passwords, students sometimes write their password on notebooks or elsewhere, thereby negating the purpose of having a password in the first place.

Finally, because some of the students are lax about protecting their passwords, other students are sometimes able to log in using passwords that are not their own. This occasionally causes problems. “We keep a log of the students’ web-surfing activities,” explains project leader Samir Hamouni, who works in the IT Department for the City of Stockholm’s Executive Office. Because the IT Department logs students’ web-surfing activities “when one student gets a little carried away in a chat room,” Hamouni says, pointing to one example, “we’ll know about it and can instruct that student on how to conduct himself when he’s surfing the web.” Naturally, the purpose of this Internet log is all for naught if students don’t use their own password.

Prior to the launch of the pilot Novell/SAFLINK solution, Kvarnbysskolan, like other Stockholm schools, was living with these problems. However, unlike other Stockholm schools, Kvarnbysskolan chose not to suffer in silence. School officials were tired of the password problems and, apparently, voiced their complaint. In fact, according to Hamouni, Kvarnbysskolan was selected to run the pilot Novell/SAFLINK solution simply

because Kvarnbysskolan “was the first to complain.” (You know what the notorious “they” always say: He who complains loudest wins.)

Hamouni and his coworkers in the IT Department for the City of Stockholm’s Executive Office noted Kvarnbysskolan’s complaint and began immediately to discuss potential solutions to the problem. From the outset, this team of engineers recognized that the only possible solution to this problem was to replace password authentication with biometric authentication. Of all of the authentication methods available—including passwords and PINs; smart cards and tokens; and biometrics—biometric methods alone are based on login factors (such as scanned fingerprints, faces, and irises) that simply cannot be forgotten. (For more information, see “Biometrics—What’s That About?” on p. 16.)

In addition, the team decided early on that fingerprint scanning would be the biometric method best suited for their needs. Specifically, fingerprint scanning is highly reliable, easy-to-use, and, compared to other biometric methods, relatively inexpensive.

Having determined the general nature of the solution they needed, the IT Department engineers launched a project, the goal of which was two-fold: The first goal was to deploy a solution to Kvarnbysskolan’s password problem. The second goal was to test this solution to determine whether it was practical for widespread deployment among other schools.

During the course of this project, the IT department for the City of Stockholm’s Executive Office took the following steps:

1. Downloaded and installed NMAS 1.0. (The IT Department plans to upgrade soon to NMAS Enterprise Edition 2.0.)
2. Evaluated two biometric vendors that support NMAS and ultimately selected SAFLINK.
3. Installed four different types of fingerprint scanners and enrolled 60 students on all four types of scanners for preliminary testing.
4. Selected and installed a single reader and then enrolled all 450 of Kvarnbysskolan’s students and teachers.

WHAT’S NMAS?

The engineers in the IT department knew that in order to use a form of authentication other than an eDirectory password, they needed NMAS. As you may know, NMAS enables organizations to expand their authentication policies.

Prior to NMAS (which was originally released in April 2000) password authentication was the only authentication method that eDirectory supported natively. Finding alternate authentication methods that worked with eDirectory was time-consuming and costly. Now, with NMAS, organizations that run eDirectory can use any authentication method they choose, including smart card, token, or biometric methods.

Kvarnbysskolan currently runs NMAS 1.0 Starter Pack (which is no longer available) but plans soon to upgrade to NMAS Enterprise Edition 2.0. NMAS Enterprise Edition 2.0 enables organizations to create login policies that may require users to authenticate using a combination of authentication methods. In other words, with NMAS Enterprise Edition 2.0, you may require users to log

Visit our advertiser, Test Out at
www.testout.com/novell.



Figure 1. Kvarnbyskolan's 80 workstations are equipped with the Liferview FingerID fingerprint scanner.

in by first entering their password, then swiping a smart card, and then scanning their fingerprint. (For an example of one organization that uses NMAS Enterprise Edition 2.0, see "Taipei County Government Secures Access to Its Assets," *Novell Connection*, Jan. 2002, pp. 24–33. You can download this article from www.ncmag.com/past.)

NMAS Enterprise Edition 2.0 also allows you to make use of graded authentication. Graded authentication is the ability to control access to the network and its resources based on authentication methods that users use. For example, you may require users to enter three login factors to access highly confidential network resources. (For more information about graded authentication, see "NMAS: It's What Spy Movies Are Made Of," *Novell Connection*, Feb. 2000, pp. 6–21. You can download this article from www.ncmag.com/past.)

NMAS Enterprise Edition 2.0 supports alternate login methods through authentication modules that Novell and third-party vendors develop. Novell-developed modules support authentication methods that use the following:

- Any X.509 v3 certificate that complies with the Public Key Cryptographic Standard (PKCS) #12
- An Entrust X.509 v3 certificate stored in the Entrust profile, a proprietary file used to encrypt and store private keys

- Smart cards from a variety of smart card vendors

(For more information about these and other Novell-developed modules, visit www.novell.com/products/nmas.)

NMAS Enterprise Edition 2.0 also supports more than 20 authentication methods from third-party vendors, including SAFLINK, RSA Security Inc., and ActivCard Inc. (For more information about these and other Novell NMAS partners, visit www.novell.com/products/nmas/partners.)

INSTALLING NMAS

To deploy NMAS 1.0, the IT Department for the City of Stockholm's Executive Office worked closely with Eterra (www.etterra.se), which has a long-term contract with the City of Stockholm. Eterra designs, builds, and operates business communications solutions for organizations in the Nordic region.

Prior to installing NMAS 1.0, the IT Department and Eterra engineers ensured that the server met the prerequisites for running this software: For example, the engineers installed Novell International Cryptographic Infrastructure (NICI) 1.5.7. (For a complete list of server minimum requirements for NMAS Enterprise Edition 2.0, visit www.novell.com/documentation/lg/nmas20.)

After upgrading the server to meet the server prerequisites, the IT Department and Eterra engineers next installed NMAS 1.0 server software and later installed NMAS client software on each of Kvarnbyskolan's 80 workstations. Before doing so, the engineers ensured that the workstations met the prerequisites, which meant, among other things, installing the Novell Client for Windows 3.30 and the NICI 1.5.7 client.

In terms of hardware configuration, the school's Windows 98 workstations, which are equipped with Pentium III or IV processors and 128 MB of RAM, more than met the client hardware prerequisites. (Workstations on which you install NMAS Enterprise Edition 2.0 client software must be running Windows 95 Release SR2B, Windows 98 SE, Windows NT with Service Pack 6a or above, or Windows 2000 Professional. These workstations must also have at least a Pentium Pro 200 processor or equivalent and a minimum of 64 MB of RAM.)

WHY SAFLINK?

Early in the project, the IT Department of the City of Stockholm's Executive Office evaluated two biometric vendors that offer NMAS modules for fingerprint authentication: Identicator Technology (www.identicator.com), a division of Identix, and SAFLINK.

The Identicator Biologon Module for NMAS from Identicator Technology and the SAFmodule for NMAS from SAFLINK are included free of charge with NMAS Enterprise Edition 2.0 (and with NMAS 1.0). Both product versions also include modules from Novell and modules from ActivCard, RSA Security, and VASCO Data Security Inc.

Ultimately, the IT Department for the City of Stockholm's Executive Office selected the SAFmodule for NMAS 2.0 from SAFLINK. NMAS Enterprise Edition 2.0 includes the server software for SAFmodule for NMAS, which enables authentication based on several different biometric technologies, including fingerprint, voice, face, and iris recognition. The client software for each of these supported biometric technologies is specific to each biometric. You must obtain this client software directly from SAFLINK and purchase user licenses. (For more information, visit www.saflink.com.)

The IT Department for the City of Stockholm's Executive Office chose the fingerprint authentication solution from SAFLINK for a number of reasons. For one thing, IT Department engineers were impressed with Data Construction, a SAFLINK distributor. Data Construction (www.dataconstruction.se) is a subsidiary of the Eiknes Group (www.eiknes.se), the largest distributor of Novell software in Sweden. Data Construction delivered all of the biometric components (including the fingerprint scanners) and provided "terrific support," says Hamouni, during all phases of this project.

In addition, the IT Department liked the fact that SAFLINK has an impressive number of biometric device partners. (For more information about these partners, visit www.saflink.com.) As a result, the IT department had the freedom to test and select from a group of several fingerprint scanners to find the scanner ideally suited for students. (For more information, see the "Testing Little Fingers" section on p. 14.)

Furthermore, the IT Department liked the idea that SAFmodule for

Visit our advertiser, CaminoSoft at
www.caminosoft.com.

Where the Pilot Runs

The Kvarnbysskolan LAN, where the Novell/SAFLINK pilot solution runs, houses 80 Windows 98 workstations, which the IT Department for the City of Stockholm's Executive Office plans to upgrade to Windows XP later this year. The school's two computer labs share approximately 40 of the workstations and the remaining 40 dot classrooms throughout the school. (See Figure 3 on p. 14.)

Kvarnbysskolan workstations are connected at 100 Mbps over copper wire to floor switches, each of which is a Cisco Catalyst 3524 XL (http://cisco.com/warp/public/cc/pd/si/casi/ca3500xl/prodliit/3500x_ds.htm.) These switches are connected at 1 Gbps over fiber optic cable that runs between floors.

The school's access switch, a Cisco Catalyst 4912G (<http://cisco.com/univercd/cc/td/doc/pcat/ca4912.htm>), connects at 1 Gbps to a switch that services all of the schools in Rinkeby, the borough (or county) where Kvarnbysskolan is located. This switch, a Cisco Catalyst 6500 (http://cisco.com/warp/public/cc/pd/si/casi/ca6000/tech/c65sp_wp.htm) connects to the Stockholm Schools Data Network core switches, all of which are Cisco Catalyst 8500 switches (<http://cisco.com/warp/public/cc/pd/si/casi/ca8500>).

In addition, the Kvarnbysskolan LAN connects to four backend Novell servers that service not only Kvarnbysskolan but

all of the schools within Rinkeby. These four servers are configured as follows:

- Two are NetWare 5.0 servers running Novell eDirectory 8.5.1. (The IT Department plans to upgrade these servers to NetWare 6 soon.)
- One is a Novell BorderManager 3.5 server. (The IT Department plans to upgrade this server to Novell BorderManager 3.7 at the same time it upgrades to NetWare 6.)
- One is a Novell GroupWise 5.5 server. (The IT Department plans to upgrade this server to GroupWise 6 at the same time it upgrades to NetWare 6.)

The Kvarnbysskolan LAN's connection to the Stockholm Schools Data Network is representative of all of the schools' connections to this city-wide WAN. Like the Kvarnbysskolan LAN, other school LANs are serviced by four Novell servers on the backend of Stockholm's other 17 boroughs. In addition, like the Kvarnbysskolan LAN, other school LANs are attached to the WAN via an access switch at the school, a switch servicing the schools in a borough, and the WAN's core routers.

In addition, the schools share a high-speed Internet connection, which provides "well over 25 Mbps" to the Internet, says Hamouni. ●

NMAS supported several biometric technologies. In fact, SAFmodule for NMAS supports 18 unique biometric authentication methods from each of four different categories of biometric technologies:

- Fingerprint scanning
- Face recognition
- Voice verification
- Iris recognition

This support for multiple biometric technologies appealed to the IT Department because it could conceive of situations where fingerprint scanning would not suffice. If the biometric alternative to passwords were to be deployed throughout the Stockholm Schools Data Network, the IT Department would need to address the physical limitations of some of the schools' children, who may not be able to press their fingers to a scanner. To this end, the IT Department is considering deploying iris-scanning devices from SAFLINK partners.

Enrolling Students in Two Easy Steps

Finally, the IT Department was impressed with SAFLINK's willingness to listen to and address their specific needs. For example, in response to the IT Department's concern about enrollment, SAFLINK en-

hanced its enrollment utility to facilitate fast enrollment of users.

Gregory Jensen, Chief Technology Officer at SAFLINK, explains that when you use biometric technology, you don't need to issue a login factor to users, because users are born with their biometric login factor. Instead, Jensen continues, you enroll users by capturing and storing in a central location their biometric data (a process also referred to as *registration*).

The user's biometric enrollment credential, Jensen explains, is called a *template*. A template is not a raw sample of the biometric factor. For example, a template of a fingerprint is not actually a fingerprint but rather a value, similar to a hash, that is derived from various characteristics of the fingerprint. Like a one-way hash, Jensen adds, biometric samples cannot be reconstructed from stored credentials. In an NMAS environment, biometric credentials are stored in the eDirectory User objects' SecretStore and are encrypted using NICI.

Because Kvarnbysskolan teachers are responsible for enrolling their students, a simple and speedy enrollment process was important. To meet this need, SAFLINK created the SAFmodule Fast Enroll utility, which enables teachers (with the appropriate rights) to enroll students in two easy steps:

1. Enter a student's eDirectory username, and click Next.
2. Ask the student to place his or her left and right index fingers (typically) on the fingerprint scanner, and click Finish.

Incidentally, SAFLINK has since included this enrollment utility in the latest version of SAFmodule, SAFmodule for NMAS 2.1.

Prior to using this utility, Kvarnbysskolan teachers used Novell's ConsoleOne to enroll students. When using ConsoleOne, teachers had to navigate the eDirectory tree to locate the User object for a particular student and then open the User object properties. Next, teachers clicked the SAFLINK Biometrics tab and, from there, clicked the Enroll button, after which they were prompted to enroll the student's fingerprints. Although this process is not difficult, the new process is faster.

More importantly, to use ConsoleOne to enroll students, the IT Department had to grant teachers full administrative rights to students' User objects. With the SAFmodule Fast Enroll utility, Jensen points out, teachers can have only limited access rights to be used "solely for the purpose of modifying students' biometric credentials."

Visit our advertiser, Novell Provisioning
at www.novell.com/e provisioning.

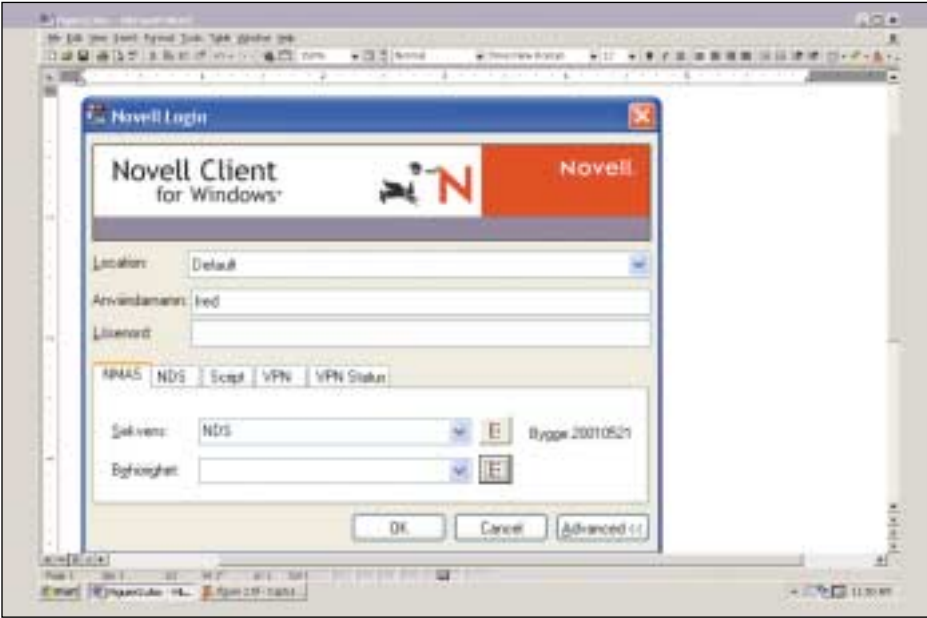


Figure 2. To log in to Stockholm Schools Data Network, Kvarnbyskolan students and teachers enter their eDirectory usernames, after which a user interface (from AuthenTec) prompts them to press their index finger to the Lifeview FingerID sensor.

Installing SAFmodule for NMAS 2.0

Having made its selection, the IT Department worked with Eterra engineers to install SAFLINK’s SAFmodule for NMAS 2.0 on Kvarnbyskolan’s NMAS server. The IT Department plans to upgrade to SAFmodule for NMAS 2.1 later this year. Among other enhancements, this upgrade will enable students to log in to workstations, whether or not the workstations have a connection to the network.

Next, the engineers installed SAFmodule for NMAS 2.0 client software on each of Kvarnbyskolan’s 80 workstations. Installing client software actually occurred in two stages: a testing phase and the actual deployment phase.

Testing Little Fingers

As you would expect, IT engineers wanted to test several fingerprint scanning devices to find the best device for the schools’ students. To this end, the IT

Department installed and tested fingerprint scanning devices from four SAFLINK partners:

- Lifeview Inc. (www.lifeview.com)
- Precise Biometrics (www.precisebiometrics.com)
- SecuGen Corp. (www.secugen.com)
- Veridicom (www.veridicom.com)

For each of these devices and, in fact, for any device that SAFmodule for NMAS supports, SAFLINK provides Biometric Service Provider (BSP) software. During the testing phase, engineers installed the appropriate BSP software for each device on 20 workstations (per device) and enrolled about 60 students, enabling each student to log in using each of the four different methods.

As is usually the case, this testing proved to be a good idea. Engineers discovered that devices from two of the vendors—Veridicom and Precise Biometrics—were well-suited for adult fingerprints but had difficulty scanning little fingers. Consequently, after approximately two months of testing, IT Department and Eterra engineers removed the software and hardware for these vendors’ devices.

Ultimately, the IT Department and Eterra engineers equipped each of Kvarnbyskolan’s 80 workstations with the Lifeview device, Lifeview FingerID. (See Figure 1 on p. 10.) Lifeview’s FingerID (www.lifeview.com/Sales/Catalog/fingerid.htm) uses AuthenTec Entrepad fingerprint sensors.

AuthenTec Technology

Through the AuthenTec BSP, SAFmodule for NMAS supports any fingerprint-scanning device that uses AuthenTec Entrepad fingerprint sensors or, more specifically, AuthenTec’s AES4000 chip. SAFmodule for NMAS supports devices from the following vendors:

- Kensington Technology Group (www.kensington.com)
- Key Source International (www.keysourceinternational.com)
- Billionton Systems Inc. (www.billionton.com.tw)
- Targus Inc. (<http://targus.com/home.asp>)
- StarTek (<http://startek.com>)

Lifeview’s FingerID actually uses AuthenTec’s AFS2 FingerLoc silicon

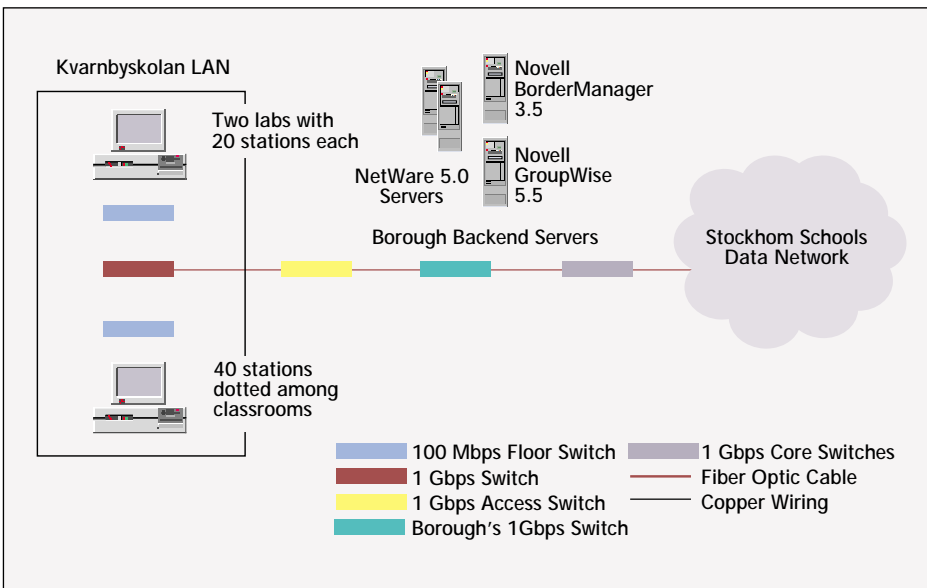


Figure 3. The Kvarnbyskolan LAN connects to the Stockholm Schools Data Network via several Cisco switches.

Do You Care?

Do you care that Kvarnbyskolan, an elementary school in Stockholm, Sweden, deployed a pilot Novell/SAFLINK biometric solution—and that it's working great? We're betting that yes, you do care—and we've got evidence to suggest that this is a safe bet.

Recently, Novell and SAFLINK Corp. jointly conducted access-and-security web seminars that more than 1,100 IT professionals attended. (Perhaps you were one of them.) During these seminars, web attendees responded to several posted survey questions. According to the as-yet unposted results, more than half of the web attendees (53 percent) indicated that they plan to replace passwords with a stronger authentication

method. Assuming this group fairly represents the rest of IT professionals, you might be interested in this case study simply because it provides one example of the successful deployment of a strong authentication method.

In addition, we think that your reasons for wanting to replace passwords, like Kvarnbyskolan's reasons, might be driven by the need for a more convenient authentication method. After all, 38.4 percent of the professionals who responded indicated that between 30 percent to 40 percent of all calls to their organization's helpdesks are for password problems. An additional 34 percent said that at least 20 percent of their helpdesk calls are for password problems. Based on these results, we think you would be interested in reading about an authentication solution that's easy enough—convenient enough—for children. ●

chip, which is fully compatible with the AES4000 chip. In fact, Jensen says, a user could be enrolled on a network using an AES4000 device. The user could then successfully log in to the network using an AFS2 device.

AuthenTec fingerprint sensors are based on AuthenTec's TruePrint technology. According to AuthenTec Inc., its TruePrint technology looks beyond

the dead surface layer of skin to the live layer underneath, where fingerprint ridge patterns, or what AuthenTec calls the "real" fingerprint, originate. (For more information about AuthenTec's TruePrint technology, visit www.authentec.com.)

In addition to this AuthenTec hardware (that is, the Entrepad fingerprint sensor), Lifeview's FingerID includes

AuthenTec fingerprint-scanning software. This AuthenTec software is responsible for the user interface that prompts a user to press his or her finger to the sensor.

Lifeview's FingerID (and other devices that use AuthenTec technology) captures and analyzes up to 15 images per second. The AuthenTec software displays these images to the user,

Visit our advertiser, Printer Properties
Pro at www.printerproperties.com.

Biometrics-What's That About?

Biometrics are big—very big. In fact, according to the International Biometric Industry Association (IBIA), biometric sales in 2001 reached U.S. \$170 million. By 2004, IBIA projects, biometric industry revenues will reach U.S. \$1 billion and by 2006, U.S. \$2 billion. (See Richard E. Norton, "Revenues Forecast for the Biometric Industry More Than Double Since Spring 2001," *Biometrics Advocacy Report*, Jan. 18, 2002 at www.ibia.org/newslett020118.htm.)

When people throw around the term *biometrics*, they're talking about each person's unique physical or behavioral characteristics that can be measured and stored, and then measured again and compared. The point of this measuring and comparing, of course, is to prove that a person is really the person he or she claims to be.

Biometrics can be used for any number of purposes (including physical admittance to buildings or verification of identities at ATMs). In the IT industry, however, the big deal about biometrics is its potential use as a secure and convenient network authentication method.

HOW DOES BIOMETRIC AUTHENTICATION WORK?

Basically, biometric authentication works by comparing what is called an *enrolled biometric sample* with a newly captured biometric sample. Making such a comparison requires four steps:

Step 1: Capture

The biometric (such as a fingerprint) is presented, and a sample is captured by a sensing device (such as a fingerprint scanner).

Step 2: Process

Distinguishing characteristics are extracted from the raw biometric sample and converted into a processed biometric identifier record (such as a fingerprint template).

Step 3: Enroll

The captured biometric record is stored in a user database for later comparison during authentication.

Step 4: Verify

A newly captured biometric record taken during login is compared against the stored record to determine if this person is who he or she claims to be.

WHAT FORMS OF BIOMETRIC AUTHENTICATION ARE AVAILABLE?

Of the biometric technologies available today, four of them are commonly used for network authentication:

- **Fingerprint Scanning.** Fingerprint scanning is the most popular biometric authentication method, probably because it is relatively fast, easy-to-use, and inexpensive. As you can guess, fingerprint authentication methods are based on capturing distinctive characteristics of the human fingerprint, such as the number of ridges between two deltas.
- **Face Recognition.** Face recognition biometric authentication methods generally require only standard off-the-shelf PC video capture cameras. These cameras typically scan the sections of

the face that are less susceptible to change. For example, they may capture raw data from the upper outlines of the eye sockets, the areas surrounding cheekbones, and the sides of the mouth.

- **Voice Verification.** Voice (or speech) verification devices focus on speech patterns that are formed by a combination of physiological and behavioral factors. These devices detect characteristics that people typically don't hear and can't impersonate.
- **Iris Recognition.** Arguably the most accurate of biometric authentication methods but also the most expensive to deploy, iris recognition is based on capturing the unique features of the human iris. Using regular or infrared light, an iris recognition device scans raw iris data searching for characteristics such as rings, furrows, and freckles.

WHY GO BIOMETRIC?

Why might you choose a biometric authentication method? Well, for one thing, biometrics are cool—James Bond cool—in addition to being convenient and secure. Not only that, but there are several inherent benefits to using a biometric (something you are) as a login factor, rather than using something you know (such as a password) or something you have (such as a smart card).

Gregory Jensen, chief technology officer at SAFLINK Corp., sums up several of the strongest arguments in favor of using a biometric as a login factor:

- You can't leave home without it.
- You can't lose it.
- You can't steal it.
- You can't forget it.
- It doesn't have to be issued.
- It doesn't have to be reissued.

You can't say the same about any other login factors—such as passwords, personal identification numbers, hardware tokens, or smart cards.

WHY NOT GO BIOMETRIC?

So what's not to like about biometric authentication methods? For one thing, they require you to install and configure some sort of device on your users' workstations. This part of biometrics is not quite as simple as just doling out passwords.

For another thing, some of your users might complain about the use of biometrics. Colleen Madigan, director of business development at SAFLINK, explains that some users worry that someone might steal their fingerprint and use it to commit a crime. Of course, you can explain to these users that the data stored is not actually a fingerprint but rather a number (a fingerprint template) from which the fingerprint cannot be reconstructed. Whether or not you can alleviate concerns that may arise isn't really the point, however: The point is, dealing with such concerns can be irritating.

On the other hand, the fact that a handful of users might complain about a new solution is not generally reason enough not to deploy that solution. What is more likely to be a significant incentive or disincentive for deploying a solution is the cost of doing so, and biometric authentication solutions have a reputation for being a bit pricey.

continued on page 18

who sees what is essentially a live videostream of his or her own fingertip images. The AuthenTec software analyzes these images to determine whether any one of them is good enough to use. Among other things, the AuthenTec software analyzes the placement of the fingertip, pressure, and clarity. Generally speaking, the Lifeview FingerID (and other devices that use the AuthenTec technology) captures a successful fingerprint image within a fraction of a second.

When the AuthenTec software determines that a suitable fingerprint image has been captured, the fingerprint images disappear, and the AuthenTec software creates a fingerprint template. This template is stored in eDirectory User objects' SecretStore. During the login process, the AuthenTec software compares a stored template with the newly captured template image and communicates to SAFmodule whether or not the two templates match. (For more information, see the "NMAS Under Cover" section on p. 18.)

INSTALLING THE DEVICES

To equip the workstations with Lifeview FingerID scanners, the IT Department and Eterra engineers completed the following steps:

1. Installed the SAFmodule for NMAS 2.0 client software (which interfaces with the NMAS client software).
2. Installed the AuthenTec BSP (which supports Lifeview FingerID and other devices).
3. Plugged Lifeview FingerIDs into the workstations' USB ports.
4. Followed the directions outlined by Lifeview FingerID's automatic installation utility, InstallShield, to load the device driver.
5. Rebooted the client.

According to Hamouni, this process took about 20 minutes per workstation, with an extra five minutes taken to enable contextless login.

Configuring NMAS

With the requisite hardware and

software installed, the IT Department and Eterra engineers configured NMAS to work with the SAFmodule for NMAS 2.0 and Lifeview FingerID scanners. First, the engineers created a Login Method object in the Kvarnbyskolan container in the city's eDirectory tree. When the engineers installed NMAS 1.0 Starter Pack, the installation program automatically created a Login Method container in the Security container in the eDirectory tree. Within this container, the engineers then created a Login Method object specifically for the SAFmodule for NMAS 2.0.

The NMAS 1.0 Starter Pack installation program also created a Login Policy container in the Security container. Engineers created a single login sequence in this container. To create this login sequence, the engineers opened the Login Policy container to view its properties and selected the General Login Sequence tab, where they created the login sequence. Engineers then selected the eDirectory rights tab to grant the necessary rights that would enable all students and teachers to use this login sequence

Visit our advertiser, Laptop Career
Certifications at www.laptopcc.com.

continued from page 16

If the supposed cost of biometrics has deterred you from investigating biometric authentication solutions, you may want to look again. The prices of biometric scanning devices—most notably fingerprint-scanning devices—have dropped considerably over the last few years. In fact, fingerprint scanning devices typically cost between only U.S. \$100 and U.S. \$130 each these days. The Lifeview FingerID scanner used at Kvarnbysskolan (the focus of this case study) is a case in point: SAFLINK lists Lifeview FingerID at U.S. \$123 per device.

Of course, the cost of the hardware device isn't the only cost of deploying a biometric authentication method. You also need to factor in software costs.

For example, suppose you choose to deploy a fingerprint authentication method on your Novell network using software from SAFLINK. First, you will need Novell Modular Authentication Service (NMAS) Enterprise Edition 2.0, which costs U.S. \$49.00 per user license. Of course, discounts are available through

licensing agreements and quantity purchases. The SAFmodule for NMAS software is similarly priced at U.S. \$49.95 per user, with discounts available for high-volume purchases.

In other words, running a fingerprint biometric authentication method on your Novell network would be available for about U.S. \$200. However, remember, this is the retail list price: Discounts are available from both SAFLINK and Novell.

A FINAL POINT TO PONDER

Whether you think this is a reasonable, low, or high price to pay for a convenient and secure authentication method, to be fair, you should consider one final point. Although issuing passwords costs nothing more than your time, how much is your time worth?

Naturally, pinning down an actual dollar amount is difficult. However, you can figure out some of the hidden costs of passwords if you think about it. For example, for most of you, anywhere from 20 percent to 40 percent of your help-desk costs are password related. (See "Do You Care?" on p. 15.) What does that cost you? That's not a rhetorical question: Think about it. ●

to log in to the Stockholm Schools Data Network.

NMAS UNDER COVER

Today, all 450 of Kvarnbysskolan's students and teachers log in daily simply by entering their username, as prompted, and then pressing either their left or right index finger to the Lifeview FingerID scanner. (Teachers enrolled students' left and right index fingers, so either will do for login.) What happens behind the scenes when a student or teacher participating in the Novell/SAFLINK pilot at Kvarnbysskolan attempts to authenticate to the network's Novell eDirectory tree?

Between the NMAS Client and the NMAS Server

Suppose student Fred has just entered his username on the initial login screen. (See Figure 2 on p. 14.) The NMAS client running on Fred's workstation stores this value in the Windows registry. When Fred clicks OK, the regular Novell client invokes the NMAS client.

On the Kvarnbysskolan network running the Novell/SAFLINK pilot, the NMAS client running on the workstation where Fred is seated establishes a connection with the NMAS server. Using NCI, the NMAS client and server create a secure pipe over which they can exchange encrypted authentication information.

The NMAS client next sends a message to the NMAS server. This message indicates all of the login methods that

have been installed on this workstation. In this case, of course, the login method is enabled by the SAFmodule for NMAS 2.0. (This module interfaces between the Lifeview FingerID scanner and NMAS.)

Novell assigns numbers to each of the login methods enabled by Novell and

“Today, all 450 of Kvarnbysskolan’s students and teachers log in daily simply by entering their username, as prompted, and then pressing either their left or right index finger to the Lifeview FingerID scanner.”

third-party authentication modules. For this example, suppose that the SAFmodule for NMAS 2.0 method is Method 1. This method, Method 1, is installed on all of the Kvarnbysskolan workstations, including the workstation where Fred is

seated. Hence, the message that the NMAS client sends to the NMAS server indicates that Fred's workstation can do Method 1.

Upon receiving this message, the NMAS server invokes the Login Server Method (LSM) associated with Method 1 (which, in this case, is the executable code for the SAFmodule for NMAS 2.0 method. This code is stored as a property of a Login Method object.) The NMAS server then sends a message to the client to DO 1 (in other words, invoke the SAFmodule for NMAS 2.0 method).

The NMAS client then loads the appropriate Login Client Method (LCM), which invokes its own Dynamic Link Library (DLL). The LSM and LCM use a protocol called Multi-Authentication Framework (MAF) to exchange, in this case, information about the SAFmodule for NMAS 2.0 method. During this process, the LCM invokes the method-specific user interface that requests the necessary login factors.

The User Interface

The user interface in this case is the AuthenTec software. This interface essentially prompts Fred to place his finger on the sensor or press Escape to cancel. After Fred duly places his finger on the Lifeview FingerID sensor, the AuthenTec software captures and analyzes images of Fred's fingerprint, images Fred can see. The AuthenTec software captures a suitable image (generally within a fraction of a second) and then creates a fingerprint template.

Using the secure channel created between the NMAS client and NICI, the SAFLINK LCM then retrieves the fingerprint template stored for Fred from eDirectory. The AuthenTec software compares the live fingerprint template against the stored fingerprint template and returns a message to the SAFLINK LCM, indicating whether the live fingerprint template matches the stored template. If the two templates match, the SAFLINK LCM returns a message to the LSM, indicating that this portion of the login sequence is completed and successful.

When Fred has completed Method 1 and his credentials have been accepted, the NMAS server confirms whether it has all of the information needed to authenticate Fred or whether more information is required. In this case, NMAS has all the information it needs because students are required only to scan their fingerprint for authentication.

If additional login methods were installed on this workstation and required for authentication, the NMAS server

would invoke the LSM for these additional methods one at a time until NMAS had confirmed that it had all of the information it needed to authenticate this user to eDirectory.

When the NMAS server is satisfied that it has all of the information it needs to authenticate Fred to eDirectory, it returns a message to the NMAS client indicating as much. The NMAS client then asks the NMAS server for Fred's credentials, and the NMAS server retrieves and returns these credentials to the NMAS client. Fred's credentials essentially indicate Fred's clearance level for this session.

The NMAS client stores these credentials (encrypted by NICI) in a secret storage on the workstation, and when Fred attempts to access information, the server on which that information is stored asks Fred's client for Fred's eDirectory credentials. As requested, the NMAS client returns Fred's encrypted credentials, at which point Fred has an authenticated connection. Although this

process may sound complex, it actually occurs within fractions of a second.

SCANNING—THE HORIZON FOR STOCKHOLM SCHOOLS

Kvarnbyskolan's password problems have been resolved once and for all—regardless of whether or not the pilot Novell/SAFLINK solution is deployed in other schools in Stockholm Schools Data Network. Ultimately, the IT Department concluded that the solution is practical for widespread deployment, but each school must decide for itself whether or not to deploy the solution. Hence, only time will tell how other Stockholm public schools resolve their respective password problems.

In the meantime, with the new Novell/SAFLINK fingerprint authentication solution, Kvarnbyskolan teachers are able to begin their computer classes right on time—every time.

Linda Kennard works for Niche Associates, an agency that specializes in writing and editing technical documents. ●

Visit our advertiser, Novell ZENworks at
www.novell.com/zenworks/promo.