You have seen the 1997 movie "Mission: Impossible"? If you have, you undoubtedly remember the scene where Ethan Hunt (the hero Tom Cruise portrays) lowers himself from a vent and downloads top-secret information while suspended above a pressure-sensitive floor. When you were watching Hollywood's depiction of life, you probably cheered for Hunt. But in your real life, you'd be more likely to cheer for the IT team responsible for securing the information Hunt is trying to steal. Why? Because you're a network administrator and protecting information is part of your job.

Granted, if you're like most network administrators, you're probably not tasked with protecting over-the-top secret information that spy movies are made of. Nevertheless, your company almost certainly has information that it wants to keep private—whether that information is government or military secrets, student or patient records, bank accounts, research files, or something as mundane as payroll data.

How do you protect this information? For starters, you probably require users to authenticate to the network, thereby ensuring that only authorized users can access network information. More specifically, you probably require users to enter Novell Directory Services (NDS) passwords to authenticate to the network. "NDS password authentication technology," says Buck Gashler, Novell product manager, "is very secure." However, Gashler concedes, "it is a password authentication scheme, and there are certain security issues with passwords."

You probably know about the security issues Gashler is referring to. No matter how many times you talk to users about creating secure passwords, enforcing your guidelines is difficult at best. How can you guarantee that not one user chooses an anniversary date or a dog's name as a password? How can you ensure that not one user writes a password on a Post-it note and sticks it under the keyboard or in a day planner? As you know only too well, you can't. Consequently, it doesn't take a spy to crack a password; it just takes one careless or indifferent user.

WHAT YOU KNOW, WHAT YOU HAVE, AND WHO YOU ARE—NDS WANTS TO KNOW

Of course, passwords are not the only secrets that users can enter to log in to a network. Passwords are an example of only one of three categories of such secrets, called login factors. The three categories of login factors are as follows:

- Something you know, such as a password
- Something you have, such as a token, public-key certificate, or smart card
- Something you are, that is, your face, fingerprint, or voice

Login methods incorporate one or more login factors from one or more of these categories. Each specific login method has unique strengths and weaknesses, and the question of which method is the most secure is highly debatable and perhaps the wrong question. (For more information about the relative strength of different login methods, see "My Way's Stronger Than Your Way!" on p. 10.)

Recognizing the security issues associated with passwords, many of you have considered using alternate login methods based on factors from the something-you-have or something-you-are categories. Some of you have even considered combining login methods from different vendors that together would require factors from two or three of these categories. Although you have considered these possibilities, most of you are still using NDS password authentication alone. Why? There are at least two probable reasons:

- Until recently, the password authentication scheme was the only scheme that NDS natively supported.
- You think that finding alternate NDS authentication schemes will take more time (and money) than you can spare.

During the last century, you may have been right. But during the first quarter of the 21st century, Novell will prove you wrong with Novell Modular Authentication Service (NMAS, pronounced en-mass) 1.0. With the NMAS client-server software and its ConsoleOne snap-in module, you can authenticate users to NDS by deploying login methods based on any type of login factor or based on a combination of factors.

SPY-STUPEFYING AUTHENTICATION

NMAS supports these login methods through several authentication modules that Novell and third-party vendors provide. In this first release, the Novell-developed authentication...
Figure 1. The level of access a user gains is based on his or her clearance and on the security label assigned to the partition and volume the user is attempting to access.

The level of access a user gains is based on the security label assigned to the partition and volume the user is attempting to access. The level of access a user gains is based on his or her clearance and on the security label assigned to the partition and volume the user is attempting to access.

Logins in Requesting Biometric & Token Clearance—Authenticated to NDS

Legend
NA = No Access
RW = Read-Write Access
R = Read-Only Access

Users can then download their certificates to a floppy diskette, a local hard drive, or even a smart card and thereafter use the certificate to authenticate to NDS via NMAS. (Smart cards are cards with computer chips that may contain a CPU and memory.)

In addition to the Novell-developed authentication modules, NMAS includes the following modules:

- A ctivity Card Module for NMAS from Acticity Card Inc.
- Identicator Biologon Module for NMAS from Identicator Technology (a division of Identix)
- RSA ACE/Agent for NMAS from RSA Security Inc.
- Secure Authentication Facility (SAF) Module for NMAS from SAFLINK Corp.
- VASCODigipass Module for NMAS from VASCO Data Security Inc.

The specific login methods these modules enable rely on a broad range of login factors, enabling authentication based on tokens, smart cards, fingerprints, voices, or faces. To deploy the methods these modules enable, you may need to purchase additional hardware or software. (For more information, see “Login Methods Worthy of Bond, James Bond” on p. 12.)

As more third-party vendors write NMAS authentication modules to enable their login methods to operate in an NMAS environment, you will have the option to install the associated software. Naturally, new NMAS authentication modules will be available from the vendors who develop them. In addition, Novell may make some of these new modules available for download on its web site.

One Little, Two Little, Three Little Methods

With this arsenal of authentication modules, NMAS enables you to create one or more company-wide authentication policies, each of which indicates a login sequence you will require for NDS authentication. These login sequences may include one or more of the login methods NMAS supports, depending on which version of NMAS you are running—NMAS Starter Pack or NMAS Enterprise Edition.

NMAS Starter Pack has been available as a free download on Novell’s web site since January 17, 2000. (You can...
My Way's Stronger Than Your Way!

When Novell developed Novell Modular Authentication Service (NMAS), "it was our conscious decision," says Hal Henderson, Novell software engineer, to take an unbiased approach. Novell "does not claim that one login method is more secure than any other login method," Henderson points out. So how do you decide which method users should use to access volumes containing information that requires varying degrees of protection?

Although the inherent overall strength of one method over another is subject to debate, each method has unique advantages and disadvantages, and you should evaluate these advantages and disadvantages before deciding which method to use. For example, password methods have the advantage of being free, and they are familiar to users and easy to use. However, passwords are often written down or poorly chosen and are, therefore, vulnerable to compromise.

Hardware tokens offer a reasonably affordable and easy-to-use alternative to passwords. Unlike passwords, which are static, hardware tokens generate dynamic passwords or one-time passwords. Hardware tokens require no software to be loaded on users' PCs and no readers (unlike smart cards). In addition, authentication methods that incorporate hardware tokens are often not always two-factor methods, requiring users to enter a Personal Identification Number (PIN) to use the token. However, hardware tokens can be lost, and many users prefer the compact size and shape of smart cards to the bulkier size and shape of tokens.

Authentication methods that incorporate smart cards are relatively easy to use and are strong, two-factor methods, requiring users to enter a PIN before using their smart card. However, authentication methods based on smart cards can be expensive to deploy because each user requires a smart card, a smart-card reader, and client software. As with tokens, users can lose or forget their smart card, and a found card can compromise security. (However, the risk of compromise is not as great as that associated with a found password because smart cards are protected by PINs.)

Methods based on biometric login factors have the unique advantage of being based on factors, such as a fingerprint, a face, or a voice, that users obviously cannot lose or forget. However, biometric authentication schemes can be quite expensive to deploy because special hardware is required. There are exceptions to this general rule. Voice authentication, for example, requires only a microphone and a sound card, which is standard equipment on most PCs.

A MATTER OF OPINION

As you would expect, the developers of login methods have differing opinions about which methods are the most and least secure. Colleen Madigan, director of marketing at SAFLINK Corp., a leading vendor of biometric authentication methods, suggests that methods based on biometrics are the most secure of any login method. "A smart card or password," Madigan says, "proves only that the person requesting access has entered the correct card or password. A biometric factor," on the other hand, "ensures that the person [requesting access] really is who he or she is claiming to be."

Other vendors' opinions differ. For example, Jean-Luc Azou, product manager at ActivCard Inc., points out what is perhaps the most common complaint about biometric login factors: These factors, like many passwords, are static. "That's the main drawback for everything that is biometric," Azou says. "Nothing guarantees," Azou continues, that a static factor—whether it is a password or a fingerprint—"cannot be reused later."

Despite differences in opinions, one opinion is shared by all vendors of login methods and by Novell: An authentication sequence that combines login methods and two or more login factors is inherently stronger than an authentication sequence based on one, single-factor login method. Combining login methods with multiple login factors, like adding bolt locks to your door, naturally increases the security of your authentication scheme.

CHOOSING THE TRUSTED PATH LESS TRAVELLED

However, before you rush out and deploy several multifactor login methods to secure the top-secret information on your company's network, consider this. No authentication method is secure if the path between the client and the authentication mechanism is not secure. "The strength of an authentication mechanism," says John Michener, senior engineer at Secure Systems Solutions, "is dependent upon the environment that it operates in. The question that we need to ask," Michener adds, "is what types of attacks is the authentication mechanism able to survive."

For example, clear-text passwords are "readily vulnerable to snooping," Michener says. While encrypted passwords are safe from snooping, they are not impervious to "a password interceptor application that is launched on the user's client and captures the user's passwords for later use," Michener points out.

"Such attacks," as Michener explains, "will defeat system or network login on insecure platforms such as Windows 95 or Windows 98. They do not work against properly implemented and installed system logins on more secure systems such as Windows NT or UNIX, where login involves the establishment of a trusted path between the authentication module and the keyboard, preventing interception from user-space Trojan attack programs."

The point is, according to Michener, if you do not ensure a trusted path between users' PCs and the authentication mechanism, regardless of the technology or number of factors you are using, "an advanced method," without a trusted path, "provides no more attack resistance than a simple username-password pair."

(For more information about trusted paths, see “Integrity of Advanced Authentication Technologies,” by John Michener and Dan Fritch, Novell development manager. You can download this article from Novell's web site at http://www.novell.com/security.)

Download NMAS Starter Pack by visiting http://www.novell.com/download and clicking “Other.” Novell also plans to bundle NMAS Starter Pack with other Novell products. Using NMAS Starter Pack, you can create one or more login sequences, each of which can be based on any one (but only one) of the login methods enabled by the NMAS authentication modules.

For example, you can create a login sequence based on the Identicator Bio-Logon Module for NMAS, which provides a fingerprint-recognition login method. Using a login sequence based on Identicator's method, users log in by placing their finger on a scanning device. (For more information about this and other...
Login Methods Worthy of Bond, James Bond

In its initial release, Novell Modular Authentication Service (NMAS) includes authentication modules from five third-party developers. Digitally signed by Novell, these modules enable users to authenticate to Novell Directory Services (NDS) using these developers’ login methods, which are based on token, smart card, and various biometric login factors. Some of these login methods require additional hardware or software, which you can purchase separately from the third-party developer.

ACTIVCARD MODULE FOR NMAS

The ActivCard Module for NMAS from ActivCard Inc. provides server software for a login method based on a smart card, a digital certificate, and a Personal Identification Number (PIN). When you use the ActivCard method in a login sequence, users log in by inserting their ActivCard Gold smart card into a smart-card reader, after which the ActivCard GUI prompts users to enter their PIN. NDS authentication is then based not only on the smart card and PIN factors but also on the user’s public-key certificate, which is stored on the ActivCard Gold smart card.

As you may have guessed, the ActivCard Module for NMAS is compatible with Novell Certificate Server 2.0.1, which is included with NMAS. Novell Certificate Server 2.0.1 stores users’ public-key certificates (and associated private keys) in NDS. You can export copies of this information directly onto users’ ActivCard Gold smart cards. This certificate may then be used for more than authentication. For example, users with ActivCard Gold smart cards can configure their e-mail programs to use the certificate stored on their smart card for exchanging encrypted and digitally signed e-mail.

In addition to the server software ActivCard Module for NMAS provides, you will need to purchase the following hardware and software from ActivCard or its authorized resellers to implement the ActivCard login method:

- ActivCard Gold (one per user), which includes client software, multiapplication smart card, and an optional smart card reader.
- ActivPack for NDS, which is a device and credential management solution. Used with NMAS, ActivPack enables network administrators to manage ActivCard Gold smart cards and the credentials stored on those cards directly from the ConsoleOne 1.2 interface.

For more information about ActivCard products, visit the ActivCard web site at http://www.activcard.com or contact ActivCard. In the United States and Canada, you can write to info@activcard.com or call 1-510-574-0100. In Europe, you can write to info@activcard.fr or call 33-1-42-04-84-00. In Asia, you can write to info@activcard.com.sg or call 65-775-3844.

IDENTIFICATOR BIOLOGON MODULE FOR NMAS

The Identicator BioLogon Module for NMAS from Identicator Technology (a division of Identix) includes client and server software that provides a login method based on a biometric factor, specifically a fingerprint. Users who log in to your company’s network using the Identicator method are prompted by the Identicator GUI to place the finger they have registered on a scanning device. This device then recognizes and records the fingerprint, which will be used to authenticate the user to NDS. The Identicator BioLogon Module for NMAS also includes management software.

To use this biometric module from Identicator you will need to purchase a scanning device that has been approved by Identicator. Approved devices are available from most computer hardware vendors and include standalone devices or devices that are integrated with a keyboard or mouse. For more information about the Identicator BioLogon Module for NMAS and Identicator-approved scanning devices, visit the Identicator web site at http://www.identicator.com or contact Identicator. You can write to info@identicator.com or call 1-408-731-2000.

Login methods NMAS supports, see “Login Methods Worthy of Bond, James Bond.”

You could also deploy a login sequence based on a two-factor login method. For example, you could create a login sequence based on RSA Security’s RSA A CE/A gent for NMAS. RSA A CE/A gent for NMAS is a two-factor login method that requires users to enter both a Personal Identification Number (PIN) and either a token or a smart card. The modules from ActivCard and VASCO also enable two-factor login methods.

Regardless of the specific login method you deploy and whether that method is a single-factor or multifactor login method, users who successfully complete a login sequence are authenticated to NDS. Beyond this first layer of security, you then control users’ access to information on your company’s network in the same way you do now, that is, through Access Control Lists (ACLs).

In other words, with NMAS Starter Pack, you are no longer limited to deploying only password-based login methods for all of your users. With NMAS Starter Pack, you can deploy different login methods for different users. You can also deploy multifactor login methods. However, with NMAS Starter Pack, you cannot combine login methods (that are enabled by different NMAS authentication modules). Also, with NMAS Starter Pack alone, you cannot control users’ access to information based on the login sequence they use to authenticate to NDS. For these capabilities, you need NMAS Enterprise Edition, which will be available for purchase beginning in March 2000.

GRADED AUTHENTICATION: HOW DID YOU GET HERE?

As with NMAS Starter Pack, NMAS Enterprise Edition enables you to create one or more authentication policies that determine the login sequences you will require for NDS authentication. However, unlike NMAS Starter Pack, which allows you to use only one login method per login sequence, NMAS Enterprise Edition enables you to combine an unlimited number of login methods for each login sequence.

For example, you could create a login sequence that combines the login

Continued on page 14
methods enabled by one of the Novell modules, by the ActiveCard module, and by the Identicator BioLogon module. This login sequence might then require users to enter an NDS password, a PIN, a smart card, and a fingerprint to be authenticated.

Although enabling you to combine your authentication methods is exciting, it is not the most exciting feature of the NMAS Enterprise Edition. It is called authentication modules, and these modules are developed, Novell assigns each module a grade. In NMAS 1.0, this grade base on the factor that a method uses. The grades for authentication modules included in NMAS 1.0 are as follows:

- Biometric & Password & Token
- Biometric & Password
- Biometric & Token
- Password & Token
- Biometric
- Password
- Token

NMAS then enables you to assign security labels to NDS partitions and NetWare volumes. The security labels, with one exception, are the same as the grades listed above. The exception is the Logged In security label.

When NMAS authentication modules are developed, Novell assigns each module a grade. In NMAS 1.0, this grade is based on the factors that a method uses. The grades for authentication modules included in NMAS 1.0 are as follows:

- Biometric & Password & Token
- Biometric & Password
- Biometric & Token
- Password & Token
- Biometric
- Password
- Token

When NMAS authentication modules are developed, Novell assigns each module a grade. In NMAS 1.0, this grade is based on the factors that a method uses. The grades for authentication modules included in NMAS 1.0 are as follows:

- Biometric & Password & Token
- Biometric & Password
- Biometric & Token
- Password & Token
- Biometric
- Password
- Token

NMAS then enables you to assign security labels to NDS partitions and NetWare volumes. The security labels, with one exception, are the same as the grades listed above. The exception is the Logged In security label.

The Logged In security label enables access without requiring the use of a specific login method. All users who have attached (but not authenticated to the network) will gain read-only rights to any partition and volume labeled Logged In. (Of course, access to NetWare volumes is still controlled through the ACLs for those volumes.) Because all NDS partitions and NetWare volumes have the Logged In label by default, you only have to label the partitions and volumes to which you want to restrict access.

The security labels you assign to particular partitions and volumes correspond to the grade of the login method you require to enable access to these partitions and volumes. For example, you can assign a Biometric & Token label to an NDS partition and NetWare volume and subsequently create a login sequence that incorporates a login method.
with a Biometric & Token grade. You can also create a login sequence that incorporates a login method with a Biometric grade and another method with a Token grade, so that the combined grade is equal to the Biometric & Token security label.

CLEAR TO GO

The whole point of assigning security labels to volumes and partitions is to enable you to increase security for parts of the network that contain sensitive information. However, labels alone will not suffice. To enforce the labels, you must also assign NDS User objects one or more clearance levels.

The names of the clearance levels you assign are identical to the names of the security labels you assign (as well as the grades Novell assigns the NMAS authentication modules). That is, you can assign User objects clearance levels such as Biometric & Password & Token, Biometric & Password, Biometric & Token, and so on. In addition, you can assign a Multi-level Adminstration clearance. Because users with Multi-level Administration have read-write access to all areas on the network, you should assign this clearance level to only a few users.

When you assign a user a particular clearance level, the user gains read-write access to the partitions and volumes with security labels that match the user’s clearance if the following are true:

- The user requests that clearance at login time.
- The user uses a method with a grade that matches his clearance level. (See Figure 1 on p. 8.)

For example, suppose a user is granted Biometric & Token clearance, requests that clearance at login, and uses a login method with a Biometric & Token grade. This user gains read-write access to partitions and volumes that have Biometric & Token labels. (See Figure 2 on p. 8.) Users do not gain access to partitions or volumes with security labels that include login factors that are not part of their clearance level. (See Figure 1 on p. 8.) For example, a user with Biometric & Token clearance cannot access volumes and partitions that are labeled Biometric & Password & Token. In addition, this user cannot access volumes and partitions that are labeled Password. (See Figure 2 on p. 8.) Users cannot access areas with security labels that are higher than or entirely different from their clearance level.

In addition, users gain read-only access to partitions and volumes with labels that require fewer but at least one of the factors named in their clearance level. (See Figure 1 on p. 8.) For example, if a user is granted Biometric & Token clearance and requests this clearance at login, this user gains read-only access to partitions and volumes labeled Biometric and partitions and volumes labeled Token. (See Figure 2 on p. 8.)

If you are wondering why a user with Biometric & Token clearance doesn’t automatically get read-write access to volumes and partitions labeled Biometric and volumes and partitions labeled Token, consider this: The more factor types you include in a login sequence, the more secure the authentication scheme.

Therefore, you will probably label partitions and volumes that hold the most confidential information with security labels that combine two or three types of login factors. You must then ensure that users with read-write access to such partitions and volumes don’t accidentally write confidential information to a volume that is less secure. To protect confidential information, NMAS grants read-only access to volumes and partitions that have labels that include the same but fewer factors than those included in users’ clearance levels.

As Dan Fritch, Novell development manager, explains, NMAS’s use of the graded authentication feature enables you, in essence, “to dynamically mount and dismount volumes and to change the mounting of the volume to read-only for a particular user session. So depending on how a user logs in,” Fritch continues, “volumes are mounted as read-write or read-only instead of being globally read-write or read-only for all users in all sessions.” In other words, with NMAS and graded authentication, you can essentially mount and dismount volumes and grant read-write or read-only access on a session-by-session basis.

MAKING THE GRADE

To run either NMAS Starter Pack or NMAS Enterprise Edition, you need a server running NetWare 5 with Support Pack 3 or above. (To download the latest support pack, visit http://support.novell.com/misc/patlst.htm#hp.) You will also need NDS 8 and Novell International Cryptographic Infrastructure (NICI) 1.5, which is included with NMAS. NICI 1.5 provides all of the cryptographic services that NMAS (and other Novell security products) requires. (For more information about NICI, see “With NICI It’s All Holes Barred,” NetWare Connection, Dec. 1998, pp. 8–20. You can download this article from http://www.nwconnection.com/past.)

To configure NMAS Starter Pack or NMAS Enterprise Edition, you need ConsoleOne 1.2, which is also included with NMAS. To enable NMAS login methods for both NMAS Starter Pack and NMAS Enterprise Edition and to
set up graded authentication (for N M A S Enterprise Edition), you use the N M A S ConsoleOne snap-in module to complete a handful of tasks. Specifically, you need to complete the first four steps listed below to configure N M A S Starter Pack, and you must complete all six steps to configure N M A S Enterprise Edition:

1. Create a Login Method container object.
2. Create a Login Policy container object.
3. Create a Login Method object.
4. Create a login sequence.
5. Apply graded authentication labels to Volume objects and partitions.
6. Apply graded authentication labels to User objects.

When you install N M A S, the Login Method container object is automatically created within the Security container object in the N D S tree. Within this Login Method container object, you create Login Method objects, one for each N ovell and third-party method that you plan to use on the network.

The Login Policy container object is also automatically created in the Security container object when you install N M A S. Within this Login Policy container object, you create one or more login sequences, which are stored as properties of the Login Policy container object.

Generally speaking, you should create at least one login sequence for each clearance level you assign. For example, if you assign Biometric & Password & Token, Biometric & Token, and Token clearance levels, you need to create at least three login sequences: One that includes methods graded Biometric, Password, and Token, another that includes methods graded Biometric and Token, and another that includes a method graded Token. However, if you also assigned a Password clearance, you would not necessarily need to create another login sequence because N M A S provides by default a sequence that includes N ovell’s password method.

You also may or may not need to create a separate login sequence for M ultilevel A dministration clearance. The sequence that users with M ultilevel A dministration clearance use must incorporate methods with grades that match the grades of all the methods in use on the network. However, this sequence does not have to incorporate all of the methods in use on the network.

For example, suppose you have some users with Password clearance logging in using a method graded Password. Further suppose that you have other users with Biometric clearance logging in using a method graded Biometric. In this case, you would need to create a separate login sequence for users with M ultilevel A dministration clearance. The new sequence would incorporate methods graded Biometric & Password but would not necessarily incorporate the same vendor-specific methods that other users are using.

To create a login sequence, you select N ew Login Sequence from the list of Available Methods field. You also may or not need to create another method graded Biometric and another method graded Token to authenticate to N D S and to gain read-write access to payroll data.

A s with every login sequence, you assign a name. In this case, let’s say you name the login sequence Payroll. To create the Payroll login sequence, you move the Biometric and Token methods listed in the Available Methods field to the Login Sequence field.

Finally, you apply graded authentication by completing the following steps: You assign security labels to the N D S partitions and N etW are volumes that hold information you want to protect, and you assign clearance levels to the U ser objects that need access to those volumes and partitions. (See Figure 4.)
When users log in to an NMA S-protected network for the first time, they enter their username and press the Advanced button on the initial login screen.

& Token label to the volume and partition that hold the payroll data. You then grant Biometric & Token clearance to the User objects associated with the users in Human Resources.

Now suppose that Leslie in Human Resources is logging in to the network for the first time or that she is requesting Biometric & Token clearance for the first time. On the initial login screen, Leslie enters her username and then selects the Advanced button. (See Figure 5.) When Leslie clicks the Advanced button, two additional fields appear: Login and Clearance. In the Login field, Leslie enters the name of the login sequence she will use, in this case Payroll. In the Clearance field, Leslie enters the clearance level that she requested last. Otherwise, Leslie enters only her username and Enter, after which the login sequence and clearance level she last entered are invoked.

NMA S UNDER COVER
You now know what a user such as Leslie sees when logging in, but what goes on behind the scenes? That is, what happens technically when a user with an NMA S-enabled client attempts to authenticate to NDS?

A ter Leslie enters her username and completes both the Login Sequence and Clearance fields on the initial login screen, the NMA S client stores these values in the Windows registry. When Leslie clicks OK, the regular Novell client invokes the NMA S client. The NMA S client searches the network to find which servers hold copies of Leslie’s User object. When the NMA S client finds these servers, it asks each one “Are you an NMA S server?” and establishes a connection with the server that responds with “Yes.” (If more than one NMA S server holds a copy of Leslie’s User object, the NMA S client randomly selects one server.) To establish this session, the NMA S client and server exchange a session key generated by NICI. This session key enables the NMA S client and server to create a secure pipe over which they can exchange encrypted authentication information.

The NMA S client next sends a message to the NMA S server. This message indicates all of the login methods that have been installed on this client. Novell assigns numbers to each of the login methods enabled by Novell and third-party authentication modules. For example, suppose that Leslie’s NMA S client has methods 5, 6, 7, and 8 installed, but Leslie is attempting to use methods 5 and 7. The message from the client indicates that Leslie’s client can do methods 5, 6, 7, and 8. This message also indicates that the login sequence Leslie requested requires method 5 be completed and then method 7.

Upon receiving this message, the NMA S server invokes the Login Server Method (LSM) associated with method 5 and then sends a message to the client to DO 5 (in other words, invoke the biometric method). The LSM is the executable code for a particular Novell or third-party authentication module. This code is stored as a property of a Login Method object.

In this case, Leslie is supposed to enter a biometric factor first, so the NMA S server invokes the biometric LSM, and the server starts running the appropriate code. When the NMA S server returns a message to the client that says DO 5, the NMA S client loads the appropriate Login Client Method (LCM), which invokes its own Dynamic Link Library (DLL). The LCM and LSM then use a protocol called Multi-Authentication Framework (MAF) to exchange the Novell or third-party method information. Novell developed MAF and has submitted an Internet-Draft titled “Multi-Authentication Framework Method for SOCKS v5” describing MAF to the Internet Engineering Task Force (IETF).

NMA S is not privy to the information that the LSM and LCM exchange via MAF. In fact, “NMA S doesn’t know what the LSM and LCM are exchanging,” says Hal Henderson, Novell software engineer, “and it doesn’t care.” During this process, the LCM invokes the method-specific user interface that requests the necessary login factors. In this case, the user interface may request that Leslie press her thumb on the fingerprint-scanning device to acquire Leslie’s fingerprint as the biometric factor used in this login method.
The LCM forwards the information Leslie enters to the LSM. The LSM compares the information it receives with the information stored in NDS to ensure that the user has entered the correct information. If Leslie really is Leslie and her biometric factor is legitimate, the LSM returns a message to the LCM, indicating this portion of the login sequence is done and successful. Both the LSM and LCM then return to NMAS.

If Leslie enters incorrect information, the NMAS server sends a message to the LCM, indicating that this portion of the login sequence is finished but unsuccessful. Leslie sees a window, indicating that her login failed. The initial login screen then appears, and Leslie can try to log in again.

When one login method is completed, the NMAS server confirms whether it has all of the information needed to authenticate Leslie or whether more information is required. In this case, Leslie must still use a token method to complete her login sequence. Consequently, the NMAS server invokes the LSM for method 7 and sends a DO 7 message to the NMAS client. The client responds by invoking the LCM for method 7, in other words, invoking the token method Leslie must complete. This process continues until the NMAS server is satisfied that it has received all of the information necessary to authenticate Leslie to NDS.

When the NMAS server is satisfied that it has received all of the information necessary to authenticate Leslie to NDS, this NMAS server returns a message to the NMAS client indicating this. The NMAS client then asks the NMAS server for Leslie's NDS credentials. The NMAS server retrieves and returns to the NMAS client Leslie's credentials, which essentially indicate Leslie's clearance level for this session.

The NMAS client then stores these credentials in a secret storage, and when Leslie attempts to access information, the server on which that information is stored asks Leslie's client for Leslie's NDS credentials. As requested, the NMAS client returns Leslie's encrypted credentials, at which point Leslie has an authenticated connection.

Although the authentication process may sound somewhat complex, this process actually occurs within fractions of a second.

NMAS AND THE RIGHT STUFF

If the IT team behind the scenes of "Mission: Impossible" had used NMAS to combine several login methods to protect the information Tom Cruise, a.k.a. Ethan Hunt, was after, the movie would have been ruined. Viewers wouldn't have been concerned with the drop of sweat that Hunt worried about. And it wouldn't have been a knife dramatically dropping to the floor that ultimately set off the alarms. Viewers would have sat bored, watching Hunt attempt in vain to steal information that was obviously inaccessible. Viewers would have known that Cruise just didn't have the face, the voice, or the smart card that he needed to get that information—even if he did have the right password.

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

For more information, visit http://www.nwconnection.com/advertise.html.

Please visit our advertiser:

SafLink Corp.

http://www.saflink.com