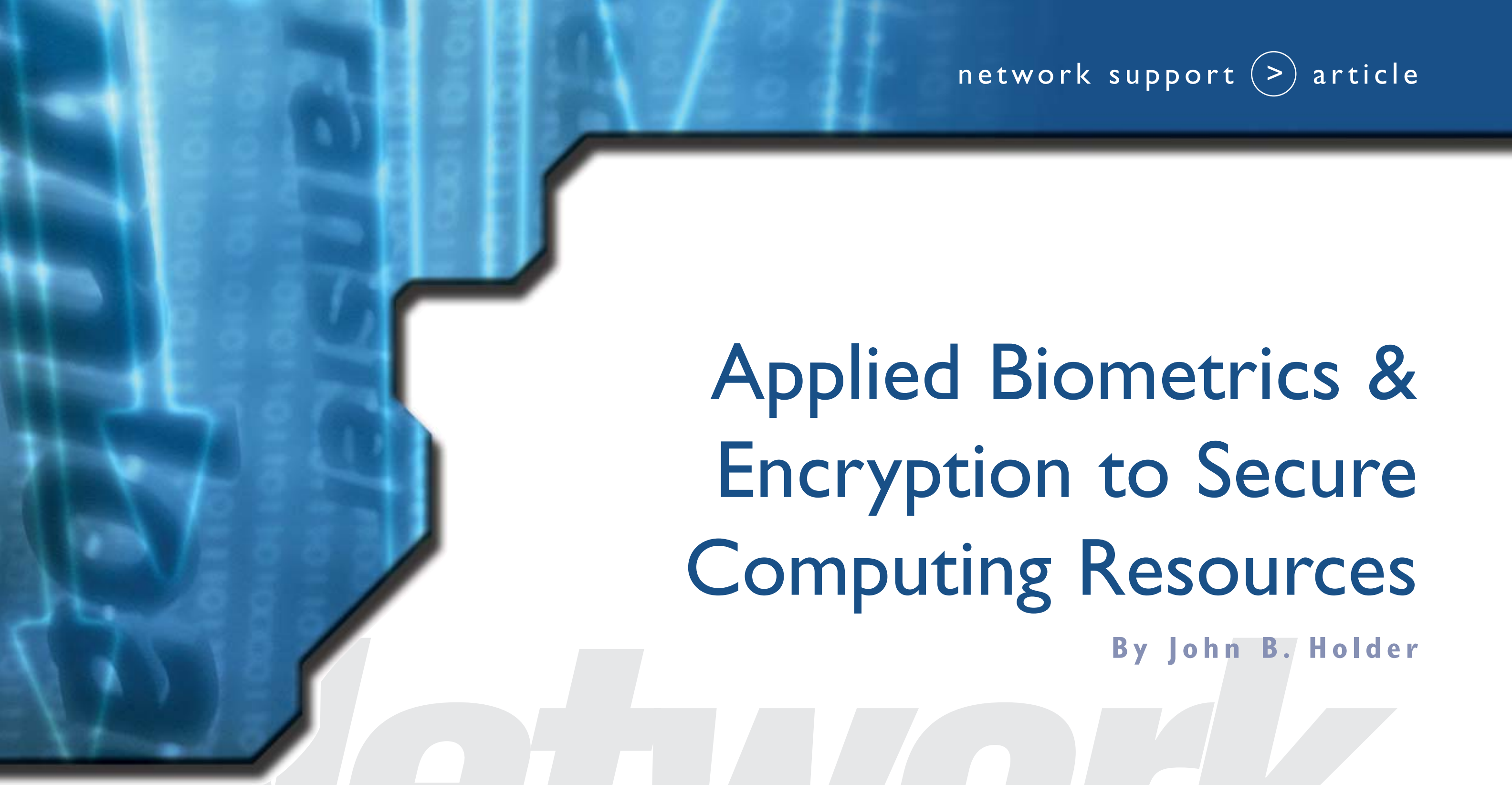


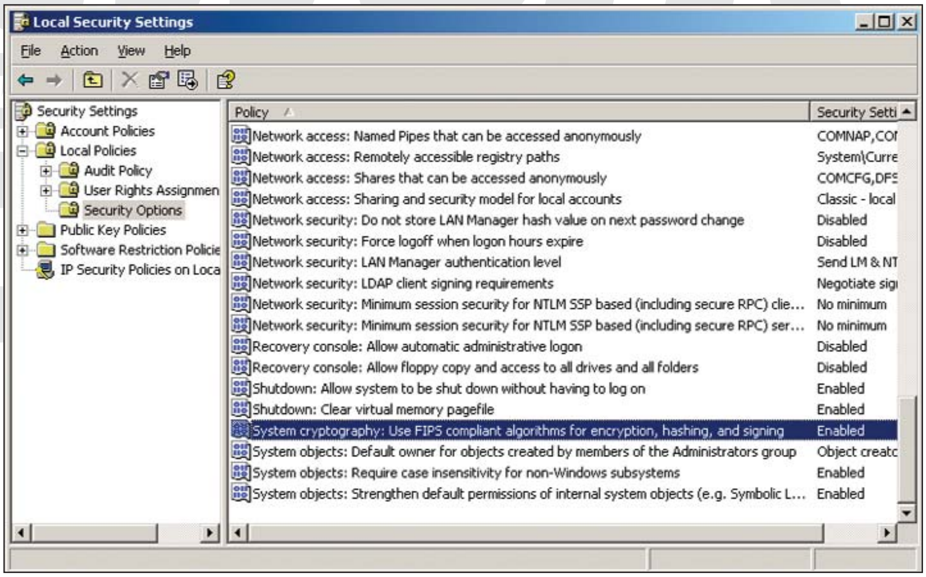
Applied Biometrics & Encryption to Secure Computing Resources

By John B. Holder

THIS article will demonstrate how to use COTS (Commercially available Off The Shelf) software & hardware to secure mobile or fixed computer systems to ensure confidentiality and protect valuable data.

Not a day goes by that information technology trade papers don't have breaking stories of a new compromise of sensitive data. These breaches of information integrity cost the industry billions of dollars each year. The trend is growing at an alarming rate, and shows no promise of changing any time soon. Modern computing has reached a level where just about everything we do on a daily basis is affected in one way or another by multitudes of computing resources. Consequently, IT professionals are faced with the reality of masses of operating system security patches, and firewall updates. They are entrusted with ensuring that all mobile & fixed computers maintain the highest levels of security for customers, donors, or employees as related to their confidentiality & protection from unauthorized access, or theft of private information.

FIGURE 1: HOW TO TURN ON ENHANCED ENCRYPTION



Policy	Security Setti
Network access: Named Pipes that can be accessed anonymously	COMNAP,COI
Network access: Remotely accessible registry paths	System\Curre
Network access: Shares that can be accessed anonymously	COMCFG,DFS
Network access: Sharing and security model for local accounts	Classic - local
Network security: Do not store LAN Manager hash value on next password change	Disabled
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Send LM & NT
Network security: LDAP client signing requirements	Negotiate sigi
Network security: Minimum session security for NTLM SSP based (including secure RPC) clie...	No minimum
Network security: Minimum session security for NTLM SSP based (including secure RPC) ser...	No minimum
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled
Shutdown: Allow system to be shut down without having to log on	Enabled
Shutdown: Clear virtual memory pagefile	Enabled
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Enabled
System objects: Default owner for objects created by members of the Administrators group	Object creatc
System objects: Require case insensitivity for non-Windows subsystems	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic L...	Enabled

There are many solutions that can be deployed, but many are very costly and hard to maintain. However, some of the newest technology solutions can be employed to make the job easier, safer, and at a minimal cost. As with any security measure, the cost of employment of a security solution should mitigate the cost of unauthorized recovery. The goal is to make it cost more to retrieve data than the unauthorized criminal is willing to pay, or spend the time to do it. This article will show you how to implement a system of Biometric log-on, and use Operating System encryption to secure your data at a reasonable cost.

GOALS & POSSIBILITIES

With the overall concept established, the ultimate goals are:

- Make unauthorized recovery too expensive for even advanced data thieves to exploit.
- Make the application of security measures user-friendly and transparent to the operators.
- Keep implementation costs under control so as to not impact daily operations budgets.

The possible solutions are:

- Increased Physical Security
- Applied Encryption
- Biometric Hardware usage for Authentication

- Vendor provided Turn-Key solutions
- Commercially available off-the-shelf hardware & software application technology

Increased physical security should be at the top of the list for any IT shop. Taking some simple steps for prevention of unauthorized disclosure or access can yield huge security benefits.

A. Develop a cohesive Information Security Policy.
B. Train employees on the proper use & storage of all computer resources and obtain acknowledgement in writing for all information security policies.
C. Provide methods of authentication for authorized users, and explore physical barriers for keeping intruders out of the workplace, and your systems.
D. Implement a sound backup policy.
E. Establish off-site storage for all backup materials.

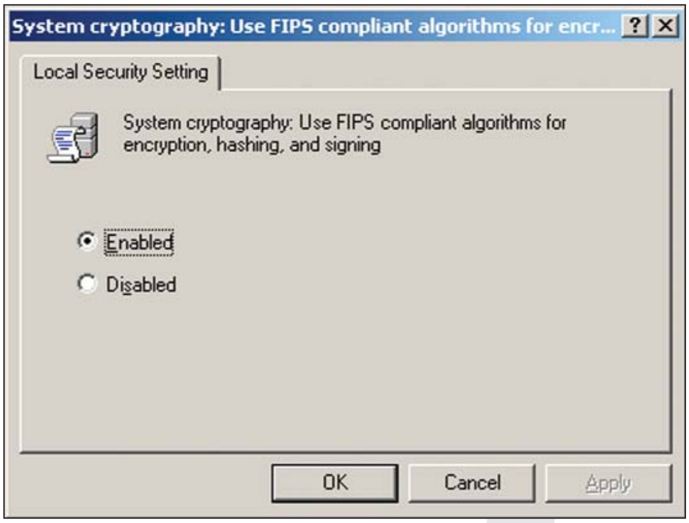
The use of encryption for sensitive data should be strongly considered. This is the second step of ensuring that confidential data stays private. It is best to go with an accepted industry standard to ensure future compatibility on any given platform. New approaches (untested encryption algorithms) can cause interoperability issues, and may cause unexpected problems or expenses. Wherever possible, it is suggested that you should use built-in capability of the underlying operating system to reduce costs and ensure future compatibility. Windows 2000 and Windows XP-Pro offer this solution, and are widely employed in this effort. Using OS provided encryption of sensitive data enables the most commonly recommended concept, “Always use a layered defense strategy.”

Biometrics has advanced to the level today that fairly inexpensive devices and software can be employed to allow a greater level of authentication than in previous years. Biometrics can enable administrators to deploy complex passwords without requiring end-users to remember them. This single facet can virtually prevent dictionary password attacks. Complex alphanumeric passwords can be employed, and can be transparent to the user.

If you desire to employ a vendor provided total biometric security solution, be prepared to pay per-user fees and possibly be impacted in added hours for administration & upkeep. Many excellent solutions are available, but they can be costly and don’t fit into every IT Department’s operating budget. This article is written for those that desire to implement custom solutions to protect their assets at a reasonable cost. Some of the available turn-key solutions can cost tens of thousands of dollars depending on the number of users you have in your organization.

As an alternative, there are several low-cost solutions that can be obtained from local resources and can be implemented with minimal administrative involvement. In this example we used the APC Biopod (biometric fingerprint reader & password manager software), and the Windows 2000/XP EFS (encrypting file system) to secure mobile computers. The cost for the Biometric devices and software in our implementation was approximately $50 per machine. The cost for the use of EFS was $0 for installed systems, and the administrative time needed to set up a system once the plan is established is less than 1 hour each. The remainder of this article will discuss that process & how it was implemented to secure mobile computing assets for a Community Blood Center in Florida.

FIGURE 2: HOW TO TURN ON ENHANCED ENCRYPTION

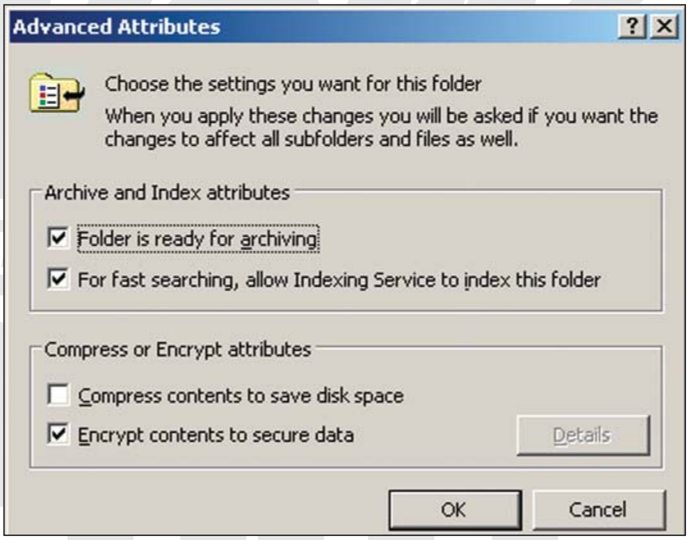

System cryptography: Use FIPS compliant algorithms for encr...

Local Security Setting

System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing

● Enabled
○ Disabled

FIGURE 3: ENCRYPTING SENSITIVE DIRECTORIES


Advanced Attributes

Choose the settings you want for this folder
When you apply these changes you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes
☑ Folder is ready for archiving
☑ For fast searching, allow Indexing Service to index this folder

Compress or Encrypt attributes
□ Compress contents to save disk space
☑ Encrypt contents to secure data

IMPLEMENTATION

System Requirements:

- Windows 2000 Professional (with high encryption pack, available online from Microsoft), or Windows XP-Pro (it is built-in).
- Pentium Class processors with > 1 GHZ speed. Pertains to Laptop computers or desktop computers depending on the application. USB 1.0/2.0 capable connections are required for recommended biometric devices.
- Physical security containers for offline storage obtained & in place. (Lockable filing cabinets, fire safes, or locked offices).
- Biometric Devices obtained in required quantities – (APC Biopod used in this example).

The first step is to enable that enhanced encryption is enabled (it is off by default). If your platform is Windows 2000, you may need to download the high-encryption pack from Microsoft’s web site. The URL for the download is: http://www.microsoft.com/windows2000/downloads/recommended/encryption/default.asp

You can also find this download by going to the Microsoft.com download area and enter the search text: “high encryption pack windows 2000.”

With Windows XP-Pro this capability is already installed & ready to implement. The following example is based on a Windows XP installation, but the Win2K implementation is similar.

HOW TO TURN ON ENHANCED ENCRYPTION

A. Open the Control Panel.
B. Open Administrative Tools.
C. Open Local Security Policy.
D. Set System Cryptography - FIPS compliant enabled. (see Figures 1 and 2)

The above setting can also be enabled as a Group Policy in a server based environment (see online operating system help for instructions on implementing group policies).

Note:

This is a fairly complex setting, so direct Windows registry edits are not recommended for enabling enhanced security. Use the security policy editor.

Ref: (1)

The Federal Information Processing Standard (FIPS) 140-1 is a security implementation validation scheme that is designed for certifying cryptographic software. FIPS 140-1 software that is validated is required by the U.S. government and requested by other prominent institutions.[1]

(Windows 2000/XP comply with this standard when enhanced security is enabled.)

ENCRYPTING SENSITIVE DIRECTORIES

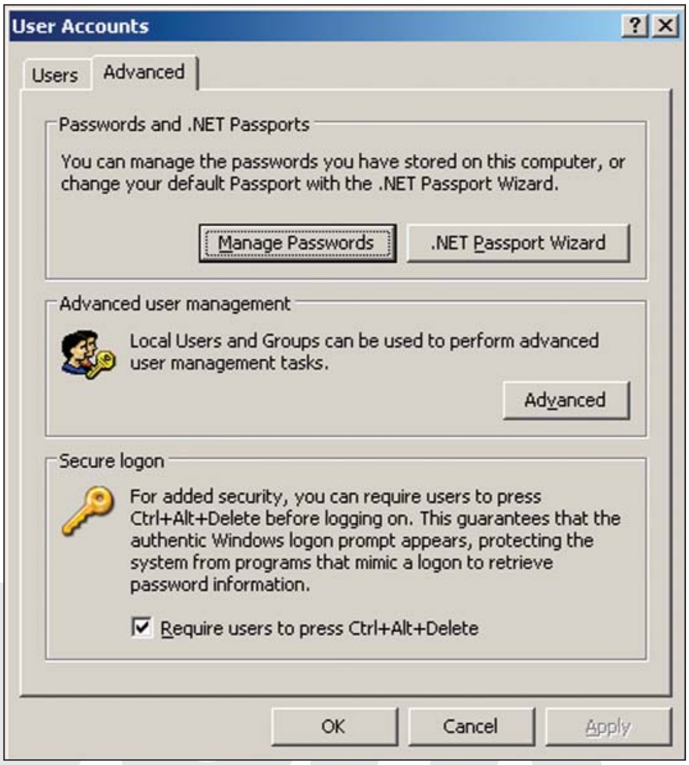
Encrypting selected directories is a relatively easy & painless process with MS Windows 2000/XP. Open the Windows Explorer, and navigate to the data directory(s) that you desire to protect. Right click on the desired folder, and click on the Advanced Button.

This dialog box allows you to select encryption to be applied to the selected directory. Please note that you can’t compress an encrypted directory. Click on OK, and allow Windows to encrypt the directory and all subdirectories. At that point you just need to assign the security (permissions) to the encrypted directory. In this manner you can allow only users that have a need to access the materials contained therein. That is accomplished by once again right clicking on the folder, and assigning the security permissions through the security tab. Group policies and permissions can be assigned to the directory if you are connected to an Active Directory network. (This does not apply to a stand alone laptop or desktop computer).

Once the FIPS compliant option is enabled and data directories are encrypted, you are ready to install & setup the biometric device(s).

Installing the APC Biopod biometric log-on and password manager is straightforward and extremely simple. Once the device is plugged in, and the software is installed all that is left to do is enroll fingerprints. In our implementation we use a common log-on for several users to gain access to a computer (laptop), and the enrollment allows for up to 20 fingerprints to be registered (through 2 log-on IDs). Each user is enrolled with a single chosen fingerprint that takes about 3 minutes. Once saved to disk in encrypted format they can log on by pressing their enrolled fingerprint on the sensor when prompted for a password.

FIGURE 4: TURNING ON SECURE LOGON OPTION



You can manage the passwords you have stored on this computer, or change your default Passport with the .NET Passport Wizard.

Local Users and Groups can be used to perform advanced user management tasks.

For added security, you can require users to press Ctrl+Alt+Delete before logging on. This guarantees that the authentic Windows logon prompt appears, protecting the system from programs that mimic a logon to retrieve password information.

☑ Require users to press Ctrl+Alt+Delete

You will need to be sure that you have the classic Windows log-on screen set as the default for the system, so that when a machine is turned on the log-on screen appears. This added security feature is accessed through the Control Panel, and User Accounts.

On the advanced tab, you need to turn on the Secure Logon option (See Figure 4).

If you want to update the Omnipass software that comes with the Biopod, you should do so before enrolling access fingerprints. Updated software can cause recognition problems with previously stored fingerprint images.

OTHER CONSIDERATIONS

Passwords: With any password selection policy, length & composition is paramount. Short passwords that can be matched with a dictionary attack should always be avoided. This simply means that if the password you have chosen can be matched against a word in a dictionary such as the examples “Feather,” or “Aardvark” then it’s not a good choice. It is best policy to use a password that is 8 or more characters in length with at least one number or punctuation mark contained within. An example variation on the above two examples would be “Fea6ther,” or “A8rdvark.” The advantage of using a biometric device to enter passwords is that they can be entered once and faithfully reproduced by the biometric device software thereby removing the necessity to remember them, and it also releases the constraints on complexity. With such a device you may choose to use passwords up to 16 characters or more in length, example “tYl34%uewacVOn198.” Just always retain a copy of assigned passwords in a separate location or stored within an encrypted library in the case they need to be manually entered if equipment fails.

Sharing & Security Model:

With some service levels of Windows the sharing & security model for local accounts is set to use the Guest account. This prevents the security tab from appearing that allows you to set individual directory permissions with the property tab within windows (seen by right clicking on a given directory within Windows Explorer & selecting properties. If this is a problem for you, just open the local policy manager (seen in FIGURE 1). A few lines above the cryptography line that was modified you'll find the key needed for modification. It is the Network Security: Sharing and security model for local accounts key. You would want to choose the Classic model that allows users to authenticate as themselves, and not the default (through Guest).

SSL Considerations:

We found what we believe to be a bug (that has been reported to Microsoft) involving the FIPS 140-1 implementation. If you choose the more robust method of encryption, hashing, and signing you will likely experience a problem with SSL. After enabling FIPS 140-1 normal 128 bit SSL connections may not function properly and any web pages that have SSL extensions may not display. Hopefully, this problem will be rectified in a forthcoming security patch. As long as the machine you are installing biometric & enhanced encryption features on doesn't need to access any SSL equipped web pages, or other SSL enabled software it won't be an issue. If you do need SSL, first test it by turning on FIPS 140-1 and then access a web page that uses SSL. If there is a problem, you can implement without the stronger method, and still retain full functionality of the biometric solution albeit at a lesser encryption key strength.

Encrypted Directories:

On one of the test systems we experienced data corruption following the changing of a password using the administrative account. Based on that one issue, I recommend that if you will be changing passwords you should use the Control + Alt + Delete function to change passwords by the designated user account. As an extra precaution, you can first decrypt any encrypted directories then change a password & re-encrypt the affected data directory.

Backups:

When backing up data from an encrypted directory over a network, or to removable medium keep in mind that once the data is copied out it will be done so in unencrypted format. You will need to provide physical security to any backup that is removed from the machine where it was encrypted. If you desire to apply encryption to backup files you will need to ensure that feature is turned on in the application you are using to conduct the backup (if available). If it is desired to do a disk-to-disk backup of encrypted directories & retain encryption, the target directory will need to be encrypted prior to starting backups, and the permissions for access will need to be pre-defined.

NaSPA member John B. Holder is the Vice President of Development at Marathon Computer Press. He has over 20 years of experience as a commercial software developer, and 25 years of experience as a network security and operations specialist. John is also the Vice President, Information Technology at Northwest Florida Blood Center, Inc., and is a member of the IEEE.

[1] FIPS 140-1 description obtained from Microsoft, and available at URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;272173