Big Sky Public Libraries: Configuring Appropriate Security

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 1 – Research on Topics in
Information Security

Submitted by: Jim Semmelroth

February 7, 2005

Small public libraries can find it difficult to keep up with managing their IT resources, particularly the security concerns. This paper provides recommendations for a small library to obtain a reasonably secure network.
Specific recommendations are made to enhance security at the perimeter, the server, and the staff and public PC's.

TABLE OF CONTENTS

Introduction …………………………….. 1
Typical Scenario …………………………….. 1
The Problem …………………………….. 2
A Little Bit of the Big Picture …………………………….. 3
Risk …………………………….. 3
CIA …………………………….. 3
Four Principles …………………………….. 4
The Risk Assessment …………………………….. 5
Valuables …………………………….. 5
Threats …………………………….. 5
Vulnerabilities …………………………….. 6
Vulnerability Mitigation …………………………….. 6
The Perimeter …………………………….. 6
All Routers …………………………….. 6
Cisco Routers …………………………….. 7
The Server …………………………….. 9
The PC's …………………………….. 15
Public PC's …………………………….. 17
Staff PC's …………………………….. 18
Wireless Hotspot …………………………….. 21
Vulnerability Testing …………………………….. 22
Continuing Education …………………………….. 23
It's a Wrap …………………………….. 24
References …………………………….. 25

Introduction

Montana is a land of big sky and small libraries. The PC and the Internet have brought substantive changes to the way these institutions provide service. A small library can easily feel caught between the need to provide whatever the latest services are and the need to provide these services with limited funding. Many library directors would be able to sleep much better at night if they simply knew they were making good technical decisions within their budget constraints.

This document purports to be good advice. This is to be read by the library director and handed to their tech support person. Portions of the document are written for the director, that she may understand the general principles supporting the specific tasks the tech support person will be engaged in. Other portions of the document are written for the tech, that he may gain a better understanding of the specific needs of a public library environment and possibly an introduction to useful tools and techniques for supporting that environment.

Typical Scenario

Consider a typical small public library in Montana. It is a Microsoft shop, partially by default, and partially because of the generosity of the Gates Foundation and the Microsoft Corporation toward Montana public libraries. Microsoft product licensing costs for public libraries are commonly less than 20% of retail. Techsoup [1] can provide some software for 4% of its retail price. Furthermore, many Montana public libraries have received PC's and network hardware from the Gates Foundation in 2000 and again in 2004.

Five souls are employed at this library for a total of 3.5 FTE. It is open 45 hours a week and is generally quite busy. None of the staff have any training on the use of PC's generally but are familiar with the tasks they need to accomplish during their workday. The library gets technical assistance from a local system/network support consultant who gives the library a generously discounted rate. The library also receives some assistance from the overworked staff at the Montana State Library.

The Public Library may have less than a dozen PC's spanning the Microsoft product line from Windows 98 to Windows XP Pro. Its Internet access is a broadband service provided by a local ISP, installed a couple years ago, configured for functionality, and hasn't been tended to since then. The library has a private address space and a single static IP address on the outside interface of its router. The server was installed many years ago, setup as a file server and the platform for the library's local electronic catalog. The OS is NT4 Server and is configured to support a domain but some clients simply run as members of a workgroup rather than authenticate against the domain server. Again, the server was configured a long time ago solely with an eye toward obtaining functionality.

The library has recently joined a consortium which shares a common database for its electronic catalog. This means that the database is kept offsite and access to it is obtained via its connection to the Internet. Thus, when access to the Internet is lost, two critical services are lost. Patrons cannot search the catalog and the library is severely limited in its ability to check-out or check-in materials.

The library provides general Internet surfing PC's to anyone who walks in. It also provides access to educational kid's games, Microsoft Office, remote databases, and the library's remote electronic catalog. It hopes to provide a wireless hotspot so patrons can bring in their own wireless-ready notebooks to get access in the library.

Most of the PC's have an antivirus program installed on them but updating signature files is done haphazardly. Similarly, the Windows update patch level varies across the PC's. The staff is becoming increasingly annoyed with the amount of SPAM they see in their inboxes, the pop-ups on their desktops, and the sluggishness of their PC's, but still are sometimes compelled to see whether they couldn't really lower their mortgage, make certain physical enhancements, or earn money at home in their sleep.

The Problem

This environment was pieced together as need or opportunity arose. It may have been done with little thought toward developing a coherent environment designed to support current and expected needs and it was almost certainly not developed with an eye toward a comprehensive security stance. The library director now recognizes she is in need of such a comprehensive vision but is unable to afford a customized security evaluation and poorly equipped to evaluate a series of proposals if such were to be presented.

The director may be thinking "I don't care about security; I just want my network to work". But the best way to get a functioning network, that stays functioning, is to design it within the context of a secure overview. Security must be incorporated into the network from the beginning. This has always been true, but has only recently become more obvious as the Internet has become much more dangerous. During the past couple years it has become much easier for an outsider, a patron, or a staff member to break the network.

Fundamentally, the library's network has two features which distinguish it. First, it is without focused, present, long-term technical support and second, it allows un-trusted users access to PC's on its subnet. This is not going to change. The library must learn how to provide reliable service with little to no technical skill on staff. Technical support is often obtained catch as catch can, but even when an individual is found appropriately skilled on system and network administration, the individual is unfamiliar with the needs peculiar to the public library environment. If that individual had a set of directions and recommendations, it would greatly facilitate the development and maintenance of a well-functioning network for the library. This document aims to be that set of recommendations.

A LITTLE BIT OF THE BIG PICTURE

Specific tasks are frequently best understood as manifestations of universal principles. To gain a better sense of why any particular task would be appropriate, a step back is useful to get a glimpse of how it fits into big picture. The specific recommendations that follow will rest on three elements of the big picture. These are the components of risk assessment, the CIA, and the four security principles. Consider each of these in turn.

RISK

A level of risk is a combination of the character of a threat and a system's vulnerability to it. Risk = Threat X Vulnerability. The level of risk decreases as either the threat or the vulnerability decreases. Since the library cannot control the threat, it must minimize risk by minimizing its vulnerability. This paper presents a list of techniques for minimizing a library's vulnerabilities. Limited funds force it to prioritize its efforts and the level of risk is the guiding principle directing those efforts.

For example, spyware is a threat. Spyware can be installed on a PC without the user's knowledge. It may look for private information, like passwords, credit card numbers, etc, and send that information to a remote site. Spyware is a big threat to casual Internet use and there is nothing a library can do about the threat, short of encouraging helpful legislation. The library can manage its vulnerability through a variety of techniques and thus lower its risk.

CIA

In this case the acronym stands for confidentiality, integrity, and accessibility. Security revolves around protecting these three areas. Each of the three components is important to any organization but different organizations emphasize the areas differently. For example, amazon.com sells stuff. If their site goes down they may be losing millions of dollars an hour, thus accessibility to their web site is the most critical of the three legs for them. On the other hand, one might think confidentiality important for a bank site because people should not see other people's account information. Even more important though, is that the bank cannot allow users to modify account data, so integrity is actually the bank's primary leg.

The public library certainly has documents that need to be kept confidential but this is not the primary component. The integrity of the electronic catalog is critical but that is now managed elsewhere by skilled individuals and can be safely left in their hands. So accessibility is the primary leg for a public library. It needs access to the Internet, access to its catalog, access to the services on the public PC's for its patrons. Access is king at the public library.

FOUR PRINCIPLES

Finally, there are four rules of thumb that should drive the tech's efforts as he prioritizes his technical efforts.

Know the system
Protection is good, but detection is a must
Principle of least privilege
Defense in depth

The admonition to know the system simply recognizes that a tech flying blind is a less effective tech. What services run on the platforms? What ports are open? What users have elevated privileges? What software is running on each platform? What policies are being enforced? What new viruses have been released recently? Knowledge about the network can be difficult to obtain and retain for the occasional tech and yet is critical.

Prudent action follows understanding and understanding is generally enhanced through observation. To be proactive, the tech should be watching what is happening on the network. That's how he would know what most needs attention. But this is generally not going to happen with the occasional tech on a small, rarely visited network. Built-in resources, such as the Event Viewer, enhance the tech's ability to collect historical data for inspection once a visit is required.

The principle of least privilege holds that people should have the means and the authority to do their job, but no more than that. It means that if a user only needs the Microsoft Word program to get their job done, then their PC and their logon is configured so that Word works but other programs don't. Similarly, the director needs to keep and maintain personnel documents, but the staff does not need to see them, so the documents are made available to the director but not to the staff.

There are two fundamentally different ways to configure restrictions. The first is to allow everything, but deny a specific set of items. The second is to deny everything, but allow a specific set of items. The principle of least privilege is an assertion of this second method.

All Montanans understand defense in depth. We can all understand the difficulties of a personal wardrobe that consists of nothing more than a pair of shorts, a tee-shirt, and a snowmobile suit good to 50 below. There are some days when this would be a good wardrobe, but there are many in-between days when this would be unsatisfactory. Threats, like the weather, come in a variety of forms and the responses should be sufficiently varied to be able to match the threat. Security will be applied across a LAN in layers. A firewall appliance may be one of the layers, but so are minor configuration settings that are cheap, easy, and do something to mitigate the vulnerabilities. Many layers will be applied for this library's security.

Armed now with many of the fundamental concepts for thinking about security, we are ready to begin the process of developing an appropriate stance.

THE RISK ASSESSMENT

An analysis of risk starts with identifying what the library has that is valuable and should be protected. Books are valuable, so the library takes the names of people who borrow them. A safe workplace is valuable so sufficient lighting and non-slip floors are tended to.

VALUABLES

Similarly, the library has valuable electronic resources. Most obviously is that information requiring privacy such as personnel documents or passwords or credit card numbers. Generally, any document that required staff time to create and would have to be re-created has value.

A second valuable resource is its access to resources. So much of what the library does requires Internet access that if this access were lost many of the services the library provides would be lost. Many services are provided on public PC's, which are unavailable if the PC isn't functioning.

A third resource is its ability to provide non-electronic related services. The librarian needs to interact with the public as a librarian. The librarian may suggest appropriate titles, answer a reference question, help a visitor identify interesting landmarks, or work with a child writing a school paper. The point is that that if they are figuring out why something isn't printing, or why a web page isn't coming up, or upgrading signature files, or updating windows, they're not being librarians, they're being geeks. The environment that lets librarians be librarians has value and should be developed and protected.

So these are the crown jewels at the library: documents, access, and librarianship. Having identified these, the next step is to ask what the threats are to these assets.

THREATS

The threat to the electronic information is anything that obtains access to them for an unauthorized use or denies access for an authorized use. Thus, they must be protected in such a manner that they cannot be lost and they are kept from any unauthorized viewing. This will be an application of the principle of least privilege.

The threat to access is more varied. An outside user can do something to break the connection to the ISP or an inside user can do something to use all available bandwidth. A patron on a public PC may bring in a worm that would infect all the other PC's, possibly disabling access to these PC's. A remote hacker may be using the library's disk storage to store illegal images.

The threats to librarianship are the same threats listed above with the addition of the threat from non-transparent technology, technology that is in your face. It is technology that will help the librarian get something done, if she could just figure out how to make it work, or once she finishes this little process. Transparent technology is the email program that lets the user process their email without having to figure out how to work the email program. Thus, in this sense, the need of an operating system for periodic patches and updates is a threat deserving of mitigation. The dynamic and increasingly dangerous Internet environment is a threat, if for no other reason than that it must be understood and its character allowed to influence behavior. To preserve the librarian's time for being a librarian, the environment needs to be hardened and self-correcting. A contemporary small network is a long way from providing transparent service, but it is a goal.

VULNERABILITIES

The vulnerabilities are too numerous to list but include Windows 98, easy passwords, open ports, uninspected logs, Windows NT, uninhibited staff, unneeded services, unmanaged patron PC's, old virus definitions, unpatched PC's, untested backups, and incorrect configurations. The list goes on.

VULNERABILITY MITIGATION

The problems requiring specific attention will be divided into distinct sections: the perimeter, the server, and the PC's. Each area has distinct vulnerabilities to be identified and treated appropriately.

THE PERIMETER

The library's perimeter is the connection to the Internet Service Provider. It is the boundary between the library's Local Area Network and the rest of the world. A small network such as this will have only a single boundary. Generically, the location is called the gateway and the device is a router. All network traffic in or out of the building traverses this router. The functionality of these routers varies greatly across vendors and models but most, if not all, would be able to perform most of the following tasks. This document recommends generic suggestions appropriate for all routers and then specific suggestions for the Cisco 827.

ALL ROUTERS

Employ the following general techniques on all routers:

- NAT: Network Address Translation allows inside hosts access to the Internet but does not allow hosts outside the LAN to see through the router to the individual PC's on the LAN. This requires that the library has at least one public IP address on the WAN interface of the router and uses an IP address space defined by RFC 1918 [2]: 10.x.x.x, 172.16-31.x.x, or 192.168.x.x.
- IP blocking: Block all access into the router from the outside that purports to be from an IP address within the address space used by the library. For example, if library is using 192.168.1.x/24 and a packet arrives at the outside port of the router with a source address of 192.168.1.x, it is probably a spoofed packet from a bad guy. Don't let it in.
- Port blocking: Microsoft OS's use ports 135, 139, and 445 for PC to PC communication on a LAN. There is no reason for anyone on the Internet to gain access to these ports. Block them at the router.
- Router Access: Limit access to the router itself. The most severe restriction would be to prohibit all access to the router except through a console port (a serial port connected to a PC running Hyperterminal). This would require the tech to be physically at the router to configure it. More common techniques are telnet and HTTP. The problem with both telnet and HTTP is that passwords are sent across the wire in clear text. Thus, if a bad guy can sniff your packets, he knows your passwords. The better option, if the router supports it, would be to use SSH instead of telnet because it encrypts the passwords. If telnet or HTTP must be used, at least restrict access to the router from only selected IP addresses, which would be the tech's management stations.
- Fault Tolerance: Routers are generally quite reliable devices, but they do fail on occasion. Consider purchasing a cheap, low-end, second router to be used simply as insurance. Configure it, verify it works, train a staff member to replace the primary with it, and put it on a shelf for use when the primary fails.
- Passwords/Pass-phrases: Never leave the router with the default passwords provided from the manufacturer. Always use a strong password and any other techniques the router supports that make it more difficult for someone to gain access to the router.
- Firmware: Keep the router's firmware level up to date. More recent firmware is generally more secure.
- Knowledge is Power: Examine the router for any other restrictions useful for slowing down the bad guys.

CISCO IOS

- Router Configurations: If the router runs Cisco IOS, the configuration for it should be saved to facilitate reconfiguration if needed. Be aware that some

Cisco passwords are trivial to decrypt. A type 7 Cisco password can be decrypted easily with a small script. Many sites provide free decryption utilities for type 7 passwords or will decrypt it online. A type 5 password is nontrivial to decrypt. Keep passwords secure by keeping the saved configuration secure.

- ACL: Obtain the IP and port blocking indicated above in Cisco IOS with an access control list or ACL. Create the extended ACL below and apply it to incoming traffic on the WAN interface. The first line assumes the LAN is 192.168.1.x. An excellent resource for the use of access lists is Sedayao [3], or online, the Cisco document “Cisco IOS Release 12.0 Network Protocols Configuration Guide, Part 1” [4].

```
access-list 101 deny ip any 192.168.1.0 0.0.0.255

access-list 101 deny tcp any any eq 135

access-list 101 deny tcp any any eq 139

access-list 101 deny tcp any any eq 445
```

This access-list would be applied to the outside interface of the router with the following command:

```
ip access-group 101 in
```

- Miscellaneous Cisco Restrictions: There are a number of other useful restrictions found in the Cisco IOS and listed below:

```
no service tcp-small-servers
no service udp-small-servers
no service finger           (newer IOS versions use “no ip finger”)
no cdp enable               (at each interface or,)
no cdp run                  (at global configuration mode)
no ip source-route
no ip directed-broadcast    (on the outside interface)
no ip redirects             (on the outside interface)
no ip unreachables          (on the outside interface)
no ip bootp server
no ip name-server
no services config
no service pad
no ip classless
```

Small servers, finger, simple network management protocol, and cisco discovery protocol are all services that are usually unneeded on a small network and have security vulnerabilities associated with them. Turn them off. The source-route and directed-broadcast commands close openings in the IOS. The redirects and unreachables commands limit what attackers can learn about the outside interface. An excellent and concise resource for learning more about these commands and other useful techniques to protect the Cisco router is "Hardening Cisco Routers" by Thomas Akin[5].

- HTTP/SNMP: Unless these services are specifically needed, HTTP and SNMP should be completely disabled. If needed, see Akin [5] to learn how to secure them. Disable with the following global commands:

  ```
  no ip http server
  no snmp-server
  ```

THE SERVER

Even a small network can benefit from the support of a server, but the server also presents a set of vulnerabilities distinct from those found at the perimeter and user PC's.

- Server 2003: The first step toward securing the server is to stop using NT 4.0. It cannot be made secure. Use only Windows 2000 server or Windows 2003 server, preferably the latter. Server 2003 Standard retails for $999 and public libraries can have it commercially for as low as $118. At TechSoup [1] it is available to public libraries for a $40 administration fee, 4% of retail.
- Patches: Apply all "critical" patches. At the time of this writing, the second Tuesday of the month is "Patch Day" at Microsoft. This is when Microsoft makes its most recent patches available. It is no longer prudent to wait a couple weeks while the rest of the world tests new patches for you. Configure the server to download and install the patches automatically. Open the Control Panel > System > Automatic Updates tab to configure this. When new Microsoft software is installed, check for new critical patches right away.
- MBSA: Use the Microsoft Baseline Security Analyzer. This tool, and useful information about it, is available at http://www.microsoft.com/technet/security/tools/mbsahome.mspx. Download and install the latest version of this tool on your server and run it against the server. It will provide a list of items and a security score associated with each item. The administrator need only examine the red and yellow scored items for a description of the inadequacy and directions for how to repair it. This tool should be run through multiple iterations continually improving the server's security level until the security assessment reports no more red or yellow flagged issues.
- DHCP: Don't use it. There are few enough hosts on the network that it is not a critical work saving feature. Not using it makes it harder for a bad guy attempting to get physical access to one of the network ports. Don't run a

DHCP server on the server or the router. Manually configure all host IP addresses. Do not allow patrons access to hot network ports. The threat presented by a patron's notebook on the library's network is substantial and should be guarded against carefully.

- Administrative Hidden Shares: Remove them. By default all drives have a hidden share. The C: drive is shared as C$, etc. The $ at the end of the share name identifies it as a hidden share which will not be shown in the browse list. For example, the command "net view \\myserver" will not show hidden shares. To see hidden shares open Administrative Tools -> Computer Management > Shared Folders > Shares. Keep only the hidden share, IPC$. Remove the others by changing (or creating) a registry entry. Open HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters and change (or create) "AutoShareServer" (REG_DWORD) to zero. Stop and restart the Server service (and dependent services) and the administrative shares will be gone. The only administrative hidden share left will be the IPC$ share, which must remain. Beware of other, similar looking, shares bad guys may have placed on the server such as IPP$ or IPS$.
- Group Policies: The library's primary user management tool is Group Policies. Mandatory on large networks, this tool is also useful for small library networks. Almost any configuration change to be made on a PC can be applied from the server with Group Policies. The following Internet sources provide a good introduction to Group Policies.

  http://www.sans.org/rr/whitepapers/windows/1374.php

  http://www.microsoft.com/technet/grouppolicy

  Upgrade Server 2003's built-in Group Policy Editor to the free Group Policy Management Console from the Microsoft download site found at http://www.microsoft.com/downloads. A very good bound reference for Group Policy is "Group Policy, Profiles, and IntelliMirror" by Jeremy Moskowitz [6].

  To make security settings for the domain controllers or for the domain, use the two tools found in "Administrative Tools" called "Domain Security Policy" and "Domain Controller Security Policy". Note that the "Default Domain Security Settings", found at Administrative Tools – Domain Security Policy, is a sub set of what is available by opening up the Group Policy Object Editor and pointing to the Default Domain Policy. A similar distinction holds for the Default Domain Controller Policy.

  Apply security settings, such as the Password Policy and the Account Lockout Policy described below, at Administrative Tools – Domain Security Policy. They won't work if applied elsewhere [6; Page 234-235].

  Active Directory must be installed to use Group Policies. Install Active Directory, DNS, and IIS (if supporting SUS). AD supports the creation of OU's (Organizational Units). An OU is a container, for users or PC's, to which policies can be applied. A set of policies may be applied to groups of users or computers by applying these policies to the OU containing the users or computers. Though a number of techniques using Group Policies are mentioned through this paper, a treatment of Group Policies cannot be provided here. All the same, understanding at least the fundamentals of its use is virtually mandatory for the tech support individual.

- Server Security: Open “Administrative Tools – Domain Controller Security Policy – Local Policies – Security Options”. Set the following options [7, Page 155-156].
    - Accounts: Guest account status: Disabled
    - Interactive logon: Do not require CTRL+ALT+DEL: Disabled
    - Microsoft network client: Digitally sign communications (if server agrees): Enabled
    - Microsoft Network server: Digitally sign communications (if client agrees): Enabled
    - Network access: Allow anonymous SID/Name Translation: Disabled
    - Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled (article 823659)
    - Network access: Do not allow storage of credentials or .NET Passports for network authentication: Enabled
    - Network access: Let Everyone permissions apply to anonymous users: Disabled
    - Network access: Sharing and security model for local accounts: Classic – local users authenticate as themselves.
    - Network security: Do not store LAN Manager hash value on next password change: Enabled
    - Network security: LAN Manager authentication level: Send LM/NTLM – Use NTLMv2 session security if negotiated.
    - Recovery Console: Allow automatic administrative logon: Disabled

  Also manually set the following registry key to a value of “2”: HKLM\System\CurrentControlSet\Control\LSA\RestrictAnonymous. This provides maximum protection from the “Null Session” attack.

- Services: Disable all unneeded services and watch for additional services the OS starts. A running service is an open port and an open port is an opportunity for the bad guys. What services are unneeded? It depends. Begin to identify unneeded services by following the advice of the MBSA. Continue with a manual inspection utilizing the informational resources found at sites such as the following:

http://www.blackviper.com

http://www.processlibrary.com

http://answersthatwork.com/Tasklist_pages/tasklist.htm

http://www.liutilities.com/products/wintaskspro/processlibrary

http://www.sysinternals.com

The BlackViper site has excellent documentation on Windows 2000/XP services and advice on which may be disabled as well as good procedural tips for removing services. The liutilities site has a list of services started up by the system, by applications, and those that are security risks.

Examine what services are running by opening Administrative Tools – Services. A service can be set to start "Automatic", "Manual", or be set to "Disabled". Test removing a service by setting it to "Disabled". Test the removal of services very carefully to avoid making the OS unable to boot.

- Accounts: The library will have 4 kinds of accounts.
  - The built-in Administrator account will have an insanely difficult password applied to it and it will be used only rarely.
  - One library staff member (probably the director) has an account with administrative rights. The tech support individual also has an account with administrative rights. If there are multiple tech support people, each will have their own account to support accountability. Never mind that the MBSA recommends only two of these accounts.
  - Staff accounts will be user-level accounts applied to the staff to support whatever functionality is needed. The director would also have a user-level account. This would be their primary account, using the administrative account only to accomplish a specific task requiring administrative privileges.
  - Public accounts will be user-level with substantial additional restrictions described below.

  All accounts will be protected with strong passwords. An exception to this rule will be described below in the public PC section. Accounts should be organized into a security group to ease assigning permissions when DACL's are configured. For example, all staff logons would be placed into a security group named "Staff". Similarly, public accounts would be placed in a security group named "Public".

  Configure the public accounts to be able to logon only at specific PC's by opening up the property sheet for the user – Account tab – Log On To… - and name the PC's that user will be allowed to logon to. Consider also doing this for the staff accounts.

- Passwords: With its password complexity requirement, Microsoft has set a minimum standard for a strong password [8], but even Microsoft recommends passwords meet a higher complexity standard. Server 2003 (and Win XP and Win 2000) support 5 settings to enforce strong passwords. Below are Microsoft's recommended values:

- Remember the last 24 passwords
- Set 42 day maximum password age
- Set 2 day minimum password age
- 8 character minimum password length
- enable password complexity requirement

Enforce Microsoft's recommendation with the following exception. Allow a 120 day maximum password age. Pity the poor librarian who just can't seem to get their password act together. In the account lockout policy, configure the following:

- 15 minute account lockout duration
- 5 attempt lockout threshold
- 5 minute lockout counter reset

Train the users to try their password 4 times. If they still fail on the 4th try, then wait 5 minutes. After 5 minutes they can try 4 times again. If they fail 5 times, then they hit the account lockout threshold and must then wait for 15 minutes before they can try again [7; Page 153]. On Server 2003, configure the Password and Account Lockout policies at Administrative Tools – Domain Security Policy – Security Settings – Account Policies.

Inform users that Windows 2000/XP/2003 supports passwords up to 127 characters in length. Encourage users to use passphrases instead of passwords because "I like 2 eat candy" is so much easier to remember than "%fd7H$uY" and increased length is the best support for strong passwords.

Remind users that password security is not primarily meant to protect staff members from other staff members. It is to protect the library from the outside world. Gaining access to the network is accomplished by decrypting passwords. Malicious sites can place spyware on PC's that sniffs and attempts to break passwords and use that information to have their way with a PC or server. One single account with an easy to break password presents a vulnerability to the whole network.

- DACL's: These are Discretionary Access Control Lists or, more simply, permissions. The server will be the repository of all the documents created and kept by the library staff because the server performs the tape backup. Although document privacy is not generally a substantial issue in this environment, the privacy of many of the director's documents certainly will be. The correct application of share and file permissions or DACL's is how private documents will be kept on a server available only to specified users.

Certainly all hosts on the network should be running NTFS, not FAT32, otherwise there is no file security.

In a representative scenario, the library would have 2 shares on the server: Common and Home. Common is a dumping area available to all staff members without restrictions. It is a way for staff to share files with each other across the network. Home would be the container for all the staff's home folders. The Home share must be available to all staff but it contains subfolders, each of which belongs to a specific staff member and available only to that staff member.

Share permissions on Common are configured by right-clicking the folder and selecting Properties > Sharing > Permissions. Permissions are applied only to the "Domain Admins" group (Full Control) and the "Staff" group (Change). No other groups or users have permissions, not "Everyone", not "System", nothing. Then file permissions are configured by right-clicking the common folder, selecting properties > security. Again apply permissions only to "Domain Admins" and "Staff". When prompted, remove the check to "Allow inheritable permissions from the parent…". This time Domain Admins will have "Full Control" and Staff will have "Modify" permissions. Thus, the Common folder is almost wide open, but only for "Staff" and "Domain Admins" accounts.

The "Home" folder is configured to support each staff member's folder being private from all other staff members. Apply Share and File permissions as above so all staff have access to the Home Share and Folder. Each staff member will then have their own subfolder in the "Home" folder. For example, the folder "Bob" will would be configured so that Bob has "Modify" permission on it and Domain Admins has "Full Control" permission. It is good to leave Domain Admins permissions on all user folders and then to configure the backup procedure to run under Domain Admins authority.

- Auditing: The MBSA recommends a set of auditing configurations. For the domain controller, set them at Administrative Tools – Domain Controller Security Policy – Local Policies – Audit Policy. Consider setting these for the Domain Security Policy as well but only if they will be inspected at the PC's. There is no point in logging the PC's if the logs are not going to be looked at. Events should be logged as follows:

Audit account logon events (Success, Failure)

Audit account management (Success, Failure)

Audit directory service access (Failure)

Audit logon events (Success, Failure)

Audit object access (Failure)

Audit privilege use (Failure)

Audit policy change (Success, Failure)

Audit system events (Success, Failure)

- Terminal Services: Terminal Services is the technique for the occasional tech to remotely manage the server (or any Windows XP box) from afar. Set the encryption level to high at the server by opening Administrative Tools - Terminal Services Configuration – Right-click the RDP-tcp icon – Properties – General Tab – Select "High" in the dropdown list.

  Teach the library staff to turn on the service only when needed with Win-Break – Remote tab – check or uncheck the box under "Remote Desktop". Also configure the router to direct port 3389 traffic to the correct private address. Disable the router from redirecting port 3389 when the project is finished.

- SUS: Software Update Services potentially allows all PC's on the LAN to obtain their updates from the local server rather than each one downloading its own update across the Internet. SUS requires IIS so all web server concerns apply. See the "Top 20 List" at http://www.sans.org/top20 to learn how to mitigate web server vulnerabilities.

  Install SUS accepting the defaults. Use IIS 6 and configure IIS to accept sessions only from LAN members. Open IIS Manager, right-click "Default Web Site" - click "Properties" – Directory Security tab – IP Address and Domain Name Restrictions – Edit - deny access to all but the entire subnet the library uses.

  Windows Update Services (WUS) is in Beta at the time of this writing. It looks to be a more feature rich product but do not use it. It requires SQL server and running SQL server on a Domain Controller is bad. Since the library only has one server, WUS is not an option.

- IIS Lockdown: Preferably run IIS 6, which is installed when 2003 server is configured to run IIS, but if running version 5 of IIS use the lockdown tool to secure the web server. The lockdown tool is available at http://www.microsoft.com/technet/security/tools/locktool.mspx.

- Common Sense: The server should not be used for general access of the Internet and no email client shall be run on it. It must be able to access the Internet to download virus signature updates, windows updates, and access the various Microsoft sites necessary to accomplish management, but no more. The server is not to be used as a user's workstation. It is not to be used as the tech's maintenance platform, except for maintenance of the LAN. If the tech can arrange to be onsite the second Tuesday of each month (Microsoft Patch Day), consider removing the default gateway on the server so that it cannot communicate outside the LAN.

THE PC'S

- OS: The first step toward adequate security in a Microsoft environment is using the right operating systems. Windows flavors 98, ME, or NT cannot be made secure. Keep them off the network. XP Home can be made sufficiently secure but is less useful because of its inability to join a domain and managed by Group Policies. Preferably, run Windows XP Professional on all staff and public PC's and Windows Server 2003 Standard on the server platform. Windows 2000 Pro and Server are suitable platforms but XP and Server 2003 should be the platforms of choice.
- Patch: The second step is maintaining the patch update status on all PC's. If the PC is also running a copy of MS Office, get the Office updates as well. Depending on the size of the library, the PC's should be configured to obtain updates from the windows update site or from a local server running SUS.
- Segregate: The network has two kinds of PC's: public and staff. It is critical that the public PC's be denied access to staff PC's completely, and to the server as much as possible. There are so many characteristics of the environment that influence the design of the topology that it's not feasible to describe them all. The most difficult decision is how to deploy the server when the network is big enough to need one. Will it be available to public PC's, staff PC's, or both? Segregation may be accomplished in a variety of ways.

  The smallest network, can use a technique called "poisoning the ARP cache". This technique disables access between appropriately configured PC's at layer 2 of the OSI model. Consider a library with two PC's, one for staff and one for the public. The IP on the staff PC is 192.168.1.5. The IP on the public PC is 192.168.1.8. At a command prompt on the staff PC, type "arp –s 192.168.1.8 00-00-00-00-00-00". Similarly, on the public PC type "arp –s 192.168.1.5 00-00-00-00-00-00". This has the effect of associating a given IP address with an invalid MAC address, thereby disabling communication. It need only be done on one of the PC's for functionality, but for layered defense do both. These commands should be placed in a batch file to be run by the PC at startup because the ARP cache is lost at shutdown.

  Use Group Policies to apply the batch file at startup, so that the ARP poisoning is applied regardless of logon. Open the GPMC. Right-click the policy in question under the "Group Policy Objects" and select "Edit". In the "Group Policy Object Editor", drill down to Computer Configuration – Windows Settings – Scripts and dbl-click "Startup" in the right pane. Use the "Add" button to bring in the batch file.

  Another segregation technique uses the VLAN capacity of a switch. Some switches can be configured to group specified ports into a "virtual LAN".

Using a switch with this feature, a set of ports can be specified for the public LAN and another set for the staff LAN, and never the two shall meet. If a server is used on the LAN, it could be made available to either or both subnets. If the switch does not support sharing the server among two VLAN's then put two NIC's in the server, one for each VLAN.

Segregation can also be accomplished at the router if the router has the capacity to route to two separate ethernets. In this case, there would be an Ethernet port on the router for the public subnet and another Ethernet port on the router for the staff subnet and traffic from one subnet to the other would be restricted. Be aware that this is not the same as simply having multiple Ethernet ports on a low-end router. This generally is a feature of more expensive routers and may not be cost effective for a small library.

- Server Service: A great technique for disabling access to a PC is simply to turn off the "Server" service on that PC. Unfortunately, it also disables useful avenues for remote management and may be more trouble than it is worth.
- Simple File Sharing: Turn it off at XP machines. Open Explorer – Tools – Folder Options… - View – Advanced Settings – uncheck "Uses Simple File Sharing (Recommended)"[9]. While there, also uncheck "Show pop-up description for folder and desktop items". If a patron machine has a desktop icon pointing to an executable in a share on the server, hovering the pointer over that icon will display the server and share name. Uncheck it and do not hand that information to patrons.
- Anti-Virus: All PC's and the server should be running an AV client and getting updates automatically from the vendor as they are made available.
- IE: Don't use it. Use Firefox 1.0. Find it at http://www.mozilla.org. Read Daniel Miessler's article "Why You Should Dump Internet Explorer" [10].

PUBLIC PC'S

- Deep Freeze: Management of public PC's proceeds along two distinct and necessary paths. First, the PC must be locked down to block common avenues of mischief. Second, it must also be designed so that any unexpected failures of the secure configuration are easily recovered from.

  A good way to accomplish this second task is a product called Deep Freeze. Deep Freeze (http://www.faronics.com) is licensed software that will "freeze' an image of a PC in a given state. All changes made after that point are rolled back at the next reboot. This means that each time the PC boots, it comes up in the same state. Everything that had changed since the reboot has been rolled back or erased. This is good for recovering from any malware a PC might have picked up or any changes a user was able to effect on a PC. It is not good for applying updated virus signatures or Windows Update patches.

Deep Freeze comes in three levels: Standard, Professional, and Enterprise. The Professional and Enterprise versions of Deep Freeze allow for maintenance windows to support making necessary changes to the PC. Thus, for example, a maintenance window would be scheduled for every Friday after the library closed. The staff would leave all the PC's on for the night. The public PC's would boot into an unfrozen state, Windows updates and virus updates could be scheduled to run automatically, or simply arranged to be performed by the staff, during that window and then the PC's would automatically boot back into a frozen state before the opening Saturday AM. Keep in mind that the PC's should not be used for general surfing during the maintenance window lest mischief be done to them.

- PACST: The Public Access Computer Security Tool from the Gates Foundation (http://pacomputing.webjunction.org/do/DisplayContent?id=7593) is a somewhat friendly and free tool used to lock down a PC so that it is kept in a fairly functional state for an extended period. On a network with no server, this tool is mandatory on public PC's. Use it.

  On a network with a server, this tool is used as the starting point for configuring policies to be distributed to the public PC's at logon. Install the PACST on a standalone PC with at least one locked down user. Identify what has been locked down by opening Administrative Tools – Policy Editor and open the policy at C:\Policy\ntconfig.pol. Manually proceed through the entire list applying the settings to a group policy being created for all public PC's on the server.

- BIOS: The BIOS interface must be password protected and the boot order must be modified to only support booting from the hard drive.
- Shares: Remove unwanted unnecessary shares as described above. The only hidden share should be IPC$. Be alert to other similarly named shares such as IPP$ or IPS$. The presence of these would suggest a back door has been introduced to the PC.
- Logon: If preferred by library staff, set the public PC's to logon automatically. Open HKLM/SOFTWARE/Microsoft/Windows NT/CurrentVersion/Winlogon. Set AutoAdminLogon to 1, and set DefaultDomainName and DefaultUserName appropriately. Configure the patron account to have no password or configure it with a password and set that with DefaultPassword. If the latter option is chosen, the password can be found in the registry in clear text. Since neither of these options is very good, opt for whatever makes the staff happy.

  The only circumstances under which an account can exist with no password is as follows:

  - Since password complexity enforcement will be disabled, manually ensure all other passwords are sufficiently strong.
  - The only PC's that accounts with no passwords can logon to are PC's

with the PASCT restrictions applied, run Deep Freeze, are segregated from Staff PC's, and the account is configured to be able to logon only at these public PC's.

STAFF PC'S

- Use SP2: The most recent service pack for Windows XP greatly improves a PC's security. Learn how to use it and modify it to support users' needs. It helps enforce the principle of least privilege.
- User Authority: When malware finds its way to a PC, it runs with the rights of the user logged on, thus it is prudent to have users run with a few rights as are needed to perform the job. Ideally, all library staff will have accounts with membership in the Domain Users security group. When the computer joins the domain, the Domain Users security group becomes a member of the local Users security group. Thus, the staff member only has "User" rights while they are logged on. That is the ideal. It is sometimes difficult for users to be able to do all they need to do with User rights and so this author has occasionally resorted to providing users with "Power User" rights on their local PC. Under no circumstances should a user be given "Domain Administrator" rights.

  When a new domain is setup, it is reasonable to want to migrate the existing user account in the workgroup to the users new domain account. This can be tricky because of ownership and permission issues. For small networks, it is much easier to simply copy needed files, such as favorites, from the old account to their respective location in the new profile.
- Executables: Group policies can be used to limit the executables able to run on a PC. The following list is the set of executables allowed to run on staff PC's in a 100+ node library. Requests from the staff for new items to be added to the list are presented only rarely.

acrobat.exe	Adobe Acrobat
acrodist.exe	Adobe Acrobat
acrord32.exe	Adobe Acrobat
calc.exe	Microsoft Calculator
catme32.exe	OCLC Application
cmd.exe	Command Prompt
conman.exe	OCLC Application
connex.exe	OCLC Application
dreamweaver.exe	Dreamweaver
excel.exe	Microsoft Office
firefox.exe	Mozilla Firefox
iexplore.exe	Internet Explorer
msaccess.exe	Microsoft Office

msohelp.exe	Microsoft Office
mspub.exe	Microsoft Office
mstore.exe	Microsoft Office
mstsc.exe	Microsoft Terminal Services
netscp.exe	Netscape Navigator
nkvbrows.exe	Nikon Camera Application
notepad.exe	Microsoft Notepad
ois.exe	Microsoft Office
outlook.exe	Microsoft Office
passport.exe	OCLC Application
powerpnt.exe	Microsoft Office
printkey2000.exe	Some users keyboard utility
psp.exe	Paint Shop Pro
realplay.exe	Real Player
rtvscan.exe	Symantec Anti-virus
sa.bat	In-house batch file
setup_wm.exe	Prep for Windows Media Player
spybotSD.exe	Spybot anti-spyware
telnet.exe	Microsoft Telnet
ultradev.exe	Dreamweaver
visio.exe	Microsoft Visio
vpc32.exe	Symantec Anti-virus
wf.bat	Workflows
wf030000.exe	Workflows
winpm-32.exe	Pegasus email client
winword.exe	Microsoft Office
wmplayer.exe	Windows Media Player
wordpad.exe	Microsoft Wordpad
ws_ftp95.exe	A popular FTP program

To configure a similar list, open the GPMC and edit the appropriate policy. Drill into User Configuration – Administrative Templates – System – “Run only allowed Windows applications”. Enable the setting and add applications. Beware. If the setting is disabled, and then re-enabled, all the applications must be re-added.

This list is not meant be restrictive to users. Any executable that may possibly be used by a staff member in the function of their daily tasks should be on the list. Enforcing this list provides some protection for the PC and the network from extraneous executables placed on the PC without the user’s knowledge. Currently, this technique, and the frequent use of a spyware scanner such as Spybot, is sufficient protection from spyware.

- Spyware: Train users to run Spybot and verify that they run it at least weekly. Alternately, it can be configured to run at startup but it is a resource hog and the PC will be unresponsive to other uses. If the library’s schedule and the hardware support the feature, a PC can be configured to automatically turn itself on 30 minutes before staff arrives, during which time various updates and scans can be run.

Just released is Beta 1 of the Microsoft Antispyware tool. At first blush, it looks promising. Microsoft is still considering the licensing and pricing for this product, as well as an enterprise version. This may be a very useful tool

- ISP: Most ISP's provide some level of protection from SPAM and viruses. Usually an account is set by default to have virus checking on and SPAM checking on but set to a permissive level. Teach users how to use these resources to their advantage.
- Physical: Attend to physical security. No patron should be allowed on staff PC's. Under no circumstances, should a patron be allowed to plug their notebook into the library's network ports. Aggressively protect network ports from attempts to do so.

  Similarly, staff should be wary about bringing their notebooks in from home and connecting them to the library network. The staff member's notebook is more easily infected at home and plugging an infected notebook into the library network puts all library PC's at risk. If this must be done, run a complete AV scan on the notebook as well as two spyware scanners before connecting it to the network. Spybot has been mentioned. Ad-Aware is another good spyware scanner that can be run on home PC's. Its license does not support its use in the library environment.
- Passwords: If you don't know how important strong passwords are yet, you're not listening.
- Temp Files: Delete the Internet Explorer temporary Internet files when IE closes: Open Internet Explorer – Tools – Internet Options – Advanced: Uncheck "Empty Temporary Internet Files folder when browser is closed". Better yet, use Firefox instead.

WIRELESS HOTSPOT

Many libraries are getting interested in setting up a wireless hotspot or Wi-Fi LAN in the library. This is useful to support patrons bringing in their own notebooks and being able to use them to access the Internet. This is a great idea from a service standpoint, but be extremely careful. Wireless access is terribly insecure. Do not setup a wireless Access Point on your LAN unless you are absolutely sure about what is being done to secure the rest of the network from the substantial vulnerabilities presented by this technology.

The best idea is simply not to set one up on the library's network at all. The library can do this and still have a hotspot. Just get a second broadband circuit into the building and connect only the wireless AP to it. Make sure there is no physical connection between the circuit brought in for the wireless hotspot and the circuit for the library's LAN. This way the library only needs to protect itself at the perimeter, which it is already doing.

The router for the hotspot should block ports 135, 139, and 445 both incoming and outgoing. This will protect patrons from some mischief coming from the Internet. It will also protect the Internet from potentially mischievous patrons in the library. Also block traffic coming from the outside purporting to have a source address in the range being used on the hotspot network. DHCP is useful for the wireless subnet so configure the router to provide IP addressing.

The helpful library staff should refrain from assisting patrons having trouble using the hotspot. From a liability standpoint, once the staff touches a patron's notebook, the library inherits every problem that notebook ever had or will have. It is easy to connect to a hotspot. Require that patrons do it themselves and advertise this requirement. Also advertise that connecting to hotspots carries risk and patrons themselves are to be held accountable for understanding the risks.

Finally, if the tech is clever, he will get the circuit for the hotspot from a different ISP than the one serving the library LAN. Thus the library has a potential failover circuit. If the first circuit goes down, chances are good that the other would still be up and available to service the library's needs instead of being used for the hotspot.

VULNERABILITY TESTING

Now look at your network as a hacker would.

- Port Scan: Run Nmap and "netstat –a" to reveal what ports are open. Take the time to learn the purpose of each open port. If it is not necessary, close it.
- Services: Take an ISC handler's advice and use Autoruns (http://www.sysinternals.com) to investigate what services are loading up. A very useful technique, for both servers and workstations, comes from Internet Storm Center handler Patrick Nolan: "In addition to Process Explorer, using the latest version of Autoruns from SysInternals allows you to show Services, select Views - enable Show Services and then

enable Hide Microsoft Signed Entries. For the remaining entries you can now highlight one and right click to Google it." [11]

- GRC.com: Run the ShieldsUp program at the Gibson Research Corporation website (http://www.grc.com). This service will scan the IP address of the router's outside interface to reveal what ports are open and thus vulnerable to compromise. On a small privately- addressed network this can be requested from any internal host. This means that any patron at any public PC with Internet access can get this information too. Close all unneeded ports.
- Null: Run the Null Session test. Open a command prompt on a PC not a member of the domain and type

  ```
  net use \\address\ipc$ “” /user:””
  ```

  Now an “Access is Denied” message should be displayed when a request to view shares is made as in the following command:

  ```
  net view \\IPaddress
  ```

- Segregation: Ping between staff and public PC's. Public PC's should not be able to get a response back from the Staff PC's and visa versa.
- Folders: Verify private folders are private. Make sure that staff logon's cannot open the director's documents folder.
- MBSA: Run the MBSA against your server. Continue to improve the server's security level until all red or yellow X's are corrected.
- Event Logs: Errors and Warnings in the System and Application event logs are indicators of areas that need attention. Use the filtering option in the Event Log viewer to look for suspicious events in the Security log. All unaccounted for logon failures should be considered suspicious. Keep in mind that the dangerous events are successful logons. In particular, successful logons from other than the staff. These would be difficult to find. Look for successful logons outside the times the library is open.
- Deep Freeze: Verify that Deep Freeze is turned on at all patron PC's before the tech leaves the building.

CONTINUING EDUCATION

Arguably, learning is the primary job function of folks working in IT. The field is so broad and dynamic that the ability to drink from a fire hose is necessary.

There are many resources available on the net to support the library tech's ascent of the learning curve. Many have been mentioned through this article. More follow.

isc.sans.org Internet Storm Center: Study this site frequently and glance at it first thing every morning.

www.sans.org The Top 20 List, SCORE, and the Reading Room will also provide a wealth of useful techniques.

www.techsoup.org This is a source of information for all things library. Techsoup Stock provides substantially discounted software for public libraries and non-profits.

pacomputing.webjunction.org The site to obtain the Public Access Computer Security Tool.

www.microsoft.com/downloads The site to download all things Microsoft.

www.sysinternals.com A great site for utilities and information supporting Windows NT/W2K/XP/2K3.

www.faronics.com See the white papers to learn how best to incorporate Deep Freeze into the library environment

IT’S A WRAP

Not really. Following these recommendations only provide a good start. Though many useful suggestions are presented, much more could potentially be done. For example, though services and group policy is touched on here, the fields are broad and worthy of substantive inspection. Note that the addition of a firewall appliance is not even mentioned. It is not that it would not be useful, but consider whether the cost of installation and maintenance of the device would be appropriate for the environment.

On the other hand, don’t be overwhelmed by the suggestions presented. Map out a plan toward better security and network functionality and use this document to help inform the plan. Continue making steps toward the goal. Think of network maintenance not so much like installing a refrigerator that sits and does what it was setup to do, but rather like doing laundry. It’s a chore that needs frequent attention.

References

1. Techsoup Stock Public Library Page. 2005. Techsoup.org. 10 Jan 2005 <http://www.techsoup.org/stock/libraries/default.asp>.

2. Internet RFC/STD/FYI/BCP Archives. 2005. Internet FAQ Archives. 10 Jan 2005 <http://www.faqs.org/rfcs/rfc1918.html>

3. Sedayao, Jeff. Cisco IOS Access Lists. Cambridge: O'Reilly & Associates, 2001.

4. Cisco IOS 12.0 Network Configuration Guide, Part 1. Cisco Press <http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_configuration_guide_chapter09186a00800b3dda.html>

5. Akin, Thomas. Hardening Cisco Routers. Cambridge: O'Reilly & Associates, 2003.

6. Moskowitz, Jeremy. Group Policy, Profiles, and Intellimirror. San Francisco: SYBEX, Inc., 2004.

7. SANS Institute. Track 1 – SANS Security Essentials. Volume 1.5. SANS Press, Jan 28, 2004.

8. Microsoft. Selecting Secure Passwords. 2005. Microsoft Small Business Center. 10 Jan 2005 <http://www.microsoft.com/smallbusiness/gtm/securityguidance/articles/select_sec_passwords.mspx>

9. Microsoft. How to configure file sharing in Windows XP. 2005. Microsoft Technet. 14 Jan 2005 <http://support.microsoft.com/kb/q304040>

10. Miessler, Daniel. Why You Should Dump Internet Explorer. 2005. LockerGnome.com. 12 Jan 2005. <http://channels.lockergnome.com/news/archives/20040615_why_you_should_dump_internet_explorer.phtml>

11. Internet Storm Center. Handler's Diary October 24 2004. 2004. SANS Internet Storm Center. 24 Oct 2004 <http://isc.sans.org/diary.php?date=2004-10-24>