SirsiDynix institute
grow your skills

upstream

Unexpected Ideas, Uncensored Opinions

FEATURING LIBRARY THOUGHT LEADERS

Marshall Breeding
Steven Carmody
Frank Cervone
Rick Cook
Erik Lewis
Ken Roberts

FALL 2005

"What are the biggest problems in network security for libraries today, and what solutions would you recommend?"

Welcome to Upstream

As an invaluable facet of the SirsiDynix Institute, the *Upstream* quarterly eZine represents another top-quality professional development tool offered at no cost to the entire library community. In addition to the SirsiDynix Institute Web Seminar Series, featuring industry thought leaders, and "Word to the Wise," a glossary designed to update you on the latest information-technology terms, *Upstream* makes an additional unique contribution.

As its subtitle suggests, *Upstream* offers unexpected ideas and uncensored opinions aimed at provoking thought, generating discussion, and fueling creative approaches to contemporary industry topics. Each issue asks an important question and includes responses from a variety of industry leaders. The result is a refreshing array of ideas, each valued for its potential to grow your skills.

SirsiDynix institute
grow your skills

Our Question

What are the biggest problems in network security for libraries today, and what solutions would you recommend?

We asked six experts—all leading thinkers in the library community—for their insight on this important topic. We are pleased to present their reactions on the following pages.

Our Thought Leaders

MARSHALL BREEDING

Library Technology Consultant and Author

Marshall Breeding is the Director for Innovative Technologies and Research at Vanderbilt University's Jean and Alexander Heard Library and a leading library technology consultant. He is a prolific author who has written or edited five books and more than 100 articles on topics including library automation, Internet technology, networking, and library trends.

As an accomplished speaker, Breeding has made more than 100 presentations to the library community through professional conferences and technology user group meetings. Online, Breeding maintains *Library Technology Guides*, a comprehensive resource and content site related to library automation, and *lib-web-cats*, a directory of libraries throughout the world.

The security threats present today seem more prevalent and pervasive than in times past. That's nothing new. The last decade or so has seen a steady escalation of attacks on the privacy and security of computer users worldwide. This environment leaves little room for error. Libraries must exercise constant vigilance to ensure the integrity of their resources and services and to protect the information that resides on their computer systems.

First, I should point out that libraries these days pay better attention to security than ever before. It's relatively rare for a library to get clobbered by a security problem. Given the unrelenting waves of attack, if libraries were not generally practicing solid security practices, the problems would be epidemic. But there is always room for improvement, and there are some areas that demand special attention.

Today, it's just not an option to run outdated and unpatched operating systems and application software. Desktop and server computers running without the latest versions of the operating system, with all security patches applied, account for the broadest set of vulnerabilities. The interval between the time that a vulnerability is discovered and when exploits emerge in the real world can be as little as a few days. We all hope that the software developer will release patches before the vulnerability can be exploited. The worst scenario involves a major vulnerability, with an active exploit in circulation, with no known patch. Fortunately, that's extremely rare.

It's essential that libraries have a proactive strategy for keeping their computers up to date. If your operating system has an automatic update feature, by all means, activate it—at least for critical security patches. Some organizations may prefer to test updates before releasing them to all their computers and might maintain a local updating service to maintain that level of control. Whether you accept updates directly from the developer or distribute them locally, get them installed across your organization expeditiously.

The second problem I see most often involves inadequate data storage strategies and disaster recovery capabilities. It's essential that no data be lost, regardless of what hardware or software failure or mishap might occur. Even when things go bad and the active version of data files are lost, backup copies exist that can easily be restored. To achieve this level of protection, it's essential that all important data be placed on well-managed storage devices. I've long recommended that libraries save all their data on file servers protected by automated daily backups, rather than allow data to be stored on local drives that are rarely, if ever, backed up. A well-managed file server provides a much higher level of security and control compared to the vagaries of having important files distributed among dozens of individual computers.

I would recommend that libraries perform a review of how they store their data files. Some of

the basic points of this review might include:

- Are all data files on servers backed up at least daily? This would include file servers, the library's ILS server, and any other database applications.
- Perform tests to ensure that files can successfully be restored from backup media.
- Audit library staff computers and review procedures to be sure that all official library data files are stored on file servers or in directories that are integrated into an automated daily backup regimen.

The third area of concern I see involves the need for a comprehensive security architecture for library networks. It's important to have multiple layers of protection against each category of threat and to have a network design where security is not an afterthought. To guard against viruses, for example, there should be filters integrated into mail servers to intercept malicious content as it enters the network, as well as the traditional anti-virus software that operates on individual computers. A well-secured network will have multiple firewalls on the network, as well as on individual systems. Often called personal firewalls, this genre of security software allows the administrator of a computer to establish detailed rules to ensure that only authorized network traffic enters or leaves the system, providing an additional thick layer of protection to supplement the network-level firewalls.

Another important aspect of a library's security architecture involves a design that separates the network traffic of public computers from that of staff computers. Library computers used by the public should be treated differently than those used by staff. Public computers pose a higher security risk, since they are used anonymously without authentication and without supervision. While libraries typically install software to lock down the computer to provide controlled access to the operating system and applications, none are completely effective.

In order to protect the staff side of the network, which includes all the data related to library operations and activities, I recommend that libraries, to the largest extent possible, isolate the traffic of all their public computers. This can be accomplished either through physical separation or by using the VLAN (Virtual Local Area Network) technology built into most Ethernet switch environments. A VLAN can make groups of computers completely invisible to each other. Having a clear line of separation between public and staff networks also makes it easy to establish a wireless hotspot without endangering the library's computing environment. A wireless LAN that connects through the public side of the network poses little or no threat to the staff side of the library network, if an effective barrier of separation has been established.

While these three topics stand out in my thinking as important security concerns, they do not comprise a comprehensive list. Each library must give careful consideration to the security of its network, continually reassessing its ability to withstand the continual barrage of attacks. It's also important that libraries not become so hamstrung by security concerns that they diminish the services they offer. It's possible to take full advantage of networked computing and offer a robust set of Web-based services for library users while still maintaining solid security.

Reach Marshall with questions or comments at:
marshall.breeding@vanderbilt.edu

STEVEN CARMODY

IT Architect at Brown University, Shibboleth Project Manager and Editor of NSF National Middleware Initiative's *Authorization Roadmap*

Steven Carmody (Brown University) is the project manager for the Shibboleth Project, part of the Internet2 MACE group, and a recognized national leader in security development related to federation and authorization strategy. He is also a member of the Internet2 MACE Steering Team, which determines direction for future Middleware infrastructure for Internet2.

Steve participates as a member of the NSF National Middleware Initiative as Editor of the *Authorization Roadmap*. For the past two years, Steve has also participated in the LionShare project as the chief technical consult for developing directions for implementation of a security strategy for P2P networks and Web Services architecture.

With the news media regularly delivering reports of computer break-ins and other security-related events, the common definition of computer security has narrowed to "protecting desktop computers from attack." Previously, however, the term had always referred to a much broader set of issues. In this article, I would like to explore potential changes in one of these other areas. That is – whether the confluence of the use of Federated Identity mechanisms for authentication, together with the expected arrival of Metasearch engines – will significantly expand the functionality available to users while improving ease of use.

Libraries provide access to a wide range of information resources. Traditionally, these resources are stored locally in hard-copy form, and the physical resource is loaned to patrons. With the widespread deployment of Internet access, however, libraries have evolved in how they deliver services to their patrons. Many resources (currently journals, increasingly eBooks) are licensed in electronic form, and made available via the Web. But access to these resources is typically controlled in some way, since their use is licensed for some defined community. Some academic libraries under budget pressure have discontinued print versions of some journals, licensing only the online version.

The advent of advanced search services, such as Google, has also impacted libraries. Google can apparently find anything – just ask my teenage daughter! Google has been immensely popular because it's easy to use from anywhere, it is very good at finding information related to a query, and its algorithms help it find very useful and valuable information (as opposed to merely documents matching the specified patterns).

We also see a growing amount of material being published from desktops, potentially becoming accessible by the search services. Currently, much of this information is only accessible via Peer-to-Peer (P2P) systems. It could, however, also be available to Google or other search engines.

We now see a world of online resources available under a variety of access constraints. Access models range from freely available – to licensed to certain communities – to taxi-meter models. One inadvertent implication of the business models associated with various online resources is the "stove-piping" of search requests. When I enter a search request, it will only traverse a small fraction of the material I am authorized to access. To do an effective search, I might have to login to a variety of different resources, navigate a variety of different search forms, and re-enter my search in a variety of different ways.

Is there a technical approach that might reduce the amount of work on a user's shoulders in order to search the relevant set of resources without having to essentially repeat the same steps with each search environment?

Two emerging technologies hold strong promise for addressing this scenario. Metasearch engines allow a search request to be entered in one place and then forwarded to a variety of other search engines. The user is often presented with a Web-based user interface that looks like a portal; the search can then span multiple databases, services, protocols, and vendors. However, the user only has to learn a single user interface. NISO is currently sponsoring a Metasearch Initiative charged with developing standards that would facilitate the ability of service providers to deploy Metasearch engines.

Federated Identity provides a "Single-Sign On" capability that spans services offered by many different organizations. Users are associated with an Identity Provider (IdP) which can be the organization they work for, the community library where their lending card is based, etc. This IdP authenticates the user for online transactions, and provides "trusted assertions" to Service Providers (SPs) about the browser user. The SPs optionally use these assertions to make access control decisions, determining which resources the user is allowed to access. These assertions would typically mean "this browser user qualifies under the terms of our contract to access this set of your resources;" thus, the SP would "trust" the IdP to be diligent about only issuing such assertions for qualifying users.

Software supporting Federated Identity is now available in the marketplace. The SAML standards promulgated by the OASIS organization (http://www.oasis-open.org/) provide the basis for interoperability between IdPs and SPs. A growing number of vendors sell software supporting this standard; the Internet2 Shibboleth project provides an open source implementation of this standard; a growing number of commercial information providers are supporting the SAML standard.

When these two technologies are combined, a user will enter a search at a single Metasearch Web site. The Metasearch engine will forward the search to a variety of open (e.g. Google) and licensed search engines. Many Higher Ed campuses, K-12 school systems, and community libraries now license online material for use by members of their communities. The user's IdP site will provide appropriate assertions to the licensed search engines. The user's search will be transparently conducted across a variety of open and licensed data repositories. At some point, assertions might be provided by multiple IdPs (corresponding to the multiple organizations that all of us are affiliated with), so that searches are conducted over the union of all repositories that all of our identities allow us access to.

Of course, this sort of security infrastructure (authentication and authorization) would have to provide a user with the ability to manage the assertion information their IdPs provide to the variety of SPs. However, this is exactly analogous to many real-world scenarios, where we decide how much or how little to tell about ourselves to others. And this is often an incremental process, as we grow our trust in the other party.

I would like to thank Peter Brantley from the University of California Digital Library Project and Oren Beit-Arie from Ex Libris for their help in exploring these ideas.

Reach Steven with questions or comments at:
steven_carmody@brown.edu

FRANK CERVONE

Assistant University Librarian for Information Technology,
Northwestern University

Frank Cervone is the Assistant University Librarian for Information Technology at Northwestern University in Evanston, IL. A prolific speaker and writer, he is the author of four books on applied information technology and has been invited to talk about library technology in Australia, Brazil, Canada, and the United Kingdom, as well as throughout the United States.

Cervone has been involved in library technology since 1992 when he joined NOTIS/Ameritech Library Services. Currently, he serves as a member of the NISO Metasearch Initiative. He holds a master's degree in Information Technology Management from DePaul University in Chicago, IL, and MSEd in Online Teaching and Learning from the California State University, East Bay, and a MBA from Northcentral University, and is currently working on a Ph.D. in Management (of Libraries) at Northcentral University.

It is hard to imagine, but there once was a time when people did not really worry much about network security. Old proprietary networking architectures, such as IBM's System Network Architecture (SNA), were designed and implemented as closed systems and were not as vulnerable to mischief as networks are today. These old networks were well defined with predetermined network routing patterns that limited the exposure of the network to external access. Even though dial-in access was possible on some networks, most network devices were "dumb" and did not have any major computational capability. Even in this protected environment, authentication was an integral component of network access.

However, that security meant you could not connect to something like Amazon.com or the local library Web site at will. Networking was effectively limited to the enterprise. Networking in the world since the widespread adoption of the Internet has enabled us to access a world of information that was previously hidden. However, that access has come at a price.

One of the initial guiding principles of the Internet networking model was that the network should be open and flexible, creating a world where network connections are created dynamically and network devices have significant and powerful computation capabilities. Access to the network was intentionally designed to be transparent and open. These decisions resulted in a network model that is very flexible, but also exposed, because there is no inherent security built into the Internet—the responsibility for security is placed solely on the machine being accessed.

As a result, most security implementations are more reminiscent of a hodgepodge of add-on products and policies rather than any coherent strategy. Not surprisingly, these products and policies tend to be based on reactive solutions, such as applying patches or using anti-virus software to look for viruses and worms. The problem with this approach is that while these solutions were effective to varying degrees in the past, they are reaching the limit of their effectiveness today. Security problems now are targeted and far more complex than ever before. Today's solutions must be proactive in order to be truly effective.

It is well worth considering—with all of the publicity related to security issues raised by the press, law enforcement, and private think tanks—what the liability of the library is related to security and security exposures. While there is no question that network attacks inconvenience the library and its patrons, the liability the library may incur because of a network security breach is a rarely discussed topic. While most librarians understand the issues related to intellectual freedom and copyright on the Internet, most have not given much consideration to the complexity of issues related to unauthorized use of data transmitted on or through the library network.

For example, most libraries have some type of privacy policy posted on their Web site, but many do not actually adhere to the promises their privacy policy makes, potentially exposing the library to legal action. Additionally, recent regulations provide strict guidelines for how information can be used. Academic libraries, for instance, that use student information run the risk of running afoul of Family Educational Rights and Privacy Act (FERPA) regulations if they do not carefully control library staff's access to student data. Furthermore, just like companies that collect and store, but do not protect, personal information, libraries risk being sued by angry patrons whose personal information has been obtained from a library-based Web site.

The potential exposure resulting from breached privacy policies is large. To date, violations of privacy and data security practices have led to actions by the Federal Trade Commission (FTC) and numerous states, as well as multi-million dollar class action lawsuits. It would be naive to assume libraries are immune.

What can a library do to address these problems? A first step is to ensure that all staff within the library is aware of the importance of security. Regular security briefings and updates should be conducted throughout the library to communicate and reinforce policy basics. Some of these basics include making sure people regularly change their passwords, do not install unauthorized applications, and ensure that physical security over laptop computers and other mobile devices is maintained.

Nevertheless, awareness is not a substitute for having a secure networking environment. An integrated approach to security involves multiple functional levels in the library from the governing board and management to IT staff and individual users. The security strategy of the library must be based on a thorough understanding of the main tenets of security technology:

- *Accountability* – proof that an intended transaction took place
- *Authenticity* – assurance that each component or person is what or who he or she says they are
- *Authority* – assurance that those who request data or information are authorized to do so
- *Availability* – provision that a system will be usable when required by the user population
- *Confidentiality* – protection of confidential information from unauthorized persons
- *Integrity* – assurance that the information sent is the same information that is received

These tenets form the basis for creating network security policies that address specific issues, such as proper use of computing resources, confidentiality of data, and procedures for dealing with a security breach. A relatively easy way to create security policies is to, instead, create procedure documents that provide detailed, step-by-step guidance for implementing various security procedures. Using this approach, the documentation regarding implementation becomes the policy itself.

In a recent InfoWorld Security Solutions survey, only 3 percent of the respondents reported their company had no formal network security policies in place. Anecdotal evidence would indicate that libraries do not fair nearly so well. However, by following the suggestions in this article, and those found in the others in this issue, a library will be in a better position to create a robust network security policy and evaluate the status of networking issues within the organization. From this position, the library will be better prepared to deal with the issues arising from the inevitable network security problems that will occur. Perhaps more importantly, with a properly designed security plan, the library will be able to avoid the many unpleasant issues related to network security by not allowing problems to occur in the first place.

Reach Frank with questions or comments at:
f-cervone@northwestern.edu

RICK COOK

Senior Technology Consultant,
SirsiDynix

Rick Cook has worked in the library automation business for 17 years—first as a network engineer for DRA and then, after a DRA-Sirsi merger, for Sirsi Corporation. During this time, Rick has overseen more than 100 customer network installations. He currently provides network consulting services to SirsiDynix customers. Prior to working in the library automation industry, Rick held various positions in information technology at a large U.S. stock brokerage firm and in the United States Air Force.

Have you installed a wireless LAN (WLAN) or are you considering a wireless installation? Have you identified how you will implement network security or staff, patron, and guest authentication? As a consultant with SirsiDynix, the number one network security issue I hear about from customers is wireless security. Many libraries spend $10,000 to $40,000 or more installing perimeter network security such as firewalls and intrusion detection. But it doesn't make much sense to spend that kind of money on security and then put up a wireless network that has little or no security, creating an easy entry point for an intruder.

SirsiDynix and Bluesocket Inc. have partnered to provide wireless security and authentication in a library environment to solve this problem I hear so much about. Bluesocket is a leader in the wireless security and authentication market. They already had a great product with many possible authentication, encryption, and management tools, but what they didn't have was the SIP2 authentication protocol. SirsiDynix has worked with Bluesocket to include SIP2 in all their wireless controllers. Now this partnership with Bluesocket enables SirsiDynix to deliver security and management to library WLANs. The wireless controllers integrate seamlessly with patron authentication servers (SIP2, radius, or others), preventing unauthorized user access, while allowing library patrons simple and secure authentication to the library's WLAN network. Library administrators can manage use by patrons by allowing or limiting access to its servers and services. They can also manage bandwidth usage on incoming and outgoing traffic to protect against the possibility that one person engaged in a high bandwidth activity (such as downloading MP3 files) could adversely affect network performance for other users. The SirsiDynix Library Wireless Hotspot solution brings the highest level of security directly to a patron's 802.11 mobile device—without requiring them to install software on their device.

The wireless controllers come in four sizes:

- BSC-400 for up to 50 simultaneous wireless users and up to eight access points
- BSC-1100 for up to 100 simultaneous users and up to 15 access points
- BSC-2100 for up to 400 simultaneous wireless users and up to 60 access points
- BSC-5000 for up to 1000 simultaneous wireless users and 100+ access points

The controllers basically have two network connections and sit between the switch supporting wireless access points and the library LAN, providing services such as Internet access. The controller "forces" wireless users to authenticate before they are allowed access to the services that the library has made available for that group of users. Roles can be configured for patrons, staff, guests, and others, with each role allowing different bandwidth management, length of the connection, and types of access, including the specific

days and times they can be connected. The solution is highly configurable.

When library patrons open a browser with their 802.11 wireless laptops, the controller presents the users with a login screen, if they are within the library's wireless access point signal. Patrons then can use their library card number and PIN number to login. For staff or guest wireless users, libraries can choose from many different types of authentication supported in the Bluesocket Controller. Any combination of authentication methods can be configured simultaneously. This is important because not all devices and operating systems have the same authentication capabilities. The Bluesocket Controller can support one or more of the following authentication methods simultaneously:

- SIP2
- Microsoft NTLM/Active Directory
- RADIUS
- LDAP
- 802.1x/WPA
- Local Controller Database
- MAC Address
- Digital Certificate
- Cisco 802.1x EAP-FAST
- Kerberos
- Cosign
- Pubcookie
- Central Authentication Server (CAS)

The controller has real-time monitoring of the Wi-Fi user's data to detect malicious traffic based on the user's actual behavior, without requiring any client-side software. This enables administrators to automatically block network access to hackers or worm infected users well before traditional signature-based tools would have updates available.

As with any network device, detailed logging and monitoring is very important. The controller supports local logging as well as Syslog. As for monitoring WLAN usage, the GUI can provide active user connection information. This active connection table displays username, IP address, MAC address, role assigned, start time, authentication type/server, and current and average bandwidth for each user.

Each Library Wireless Hotspot configuration is unique and based on the wants and needs of that organization. SirsiDynix has "core configuration" Library Wireless Hotspots where one or more large controllers are installed at the central site supporting all wireless access points, including those at remote (across the WAN) libraries. This scenario works best when used with the Bluesocket AP-1500 Access Points that automatically find the controller on the network and auto-configure. A more common scenario is to install the solution in a "distributed configuration" where there are smaller controllers at each library. The SirsiDynix Library Wireless Hotspot solution provides robust wireless management and security, regardless of network size.

With SirsiDynix, you won't have to worry about staying ahead of the wireless security game, because you'll have the full strength of the industry's leader in library automation behind you with our array of innovative products. With more than 15 years of networking experience, SirsiDynix can provide hardware equipment and services that are ideally configured for your library environment. Whether it's consulting services, equipment refreshing, or end-to-end network or security solutions, SirsiDynix can exceed your networking expectations. For more information, call 866-805-5815 or email sales@sirsidynix.com.

Reach Rick with questions or comments at:
rick.cook@sirsidynix.com

ERIK LEWIS

Resources Coordinator/Technology Supervisor,
Northwest Georgia Regional Library System

Lewis' experience includes working in technology at the state and local library levels, working for a library automation vendor, as well as a myriad of technical training courses. He helped start TechTalk, the first technology listserv for libraries in the state of Georgia and now provides network and security consulting to several library systems.

Mr. Lewis holds a master's degree in library science from Clarion University and an undergraduate degree from West Virginia University. He lives in Cartersville, GA, with his wife and a trio of small yappy dogs. In his spare time, he consults on technology, purchasing, security, planning and audits.

Every week, new reports surface of security breaches that release the private details of a few million credit card accounts. From the stealing of credit card information affecting millions to a ring of thieves stealing from neighborhood mailboxes, identity theft continues to grow. Every day that a library isn't involved is borrowed time. The reason? Despite this rapidly growing, highly publicized type of crime, libraries continue to record Social Security numbers, driver's license numbers, and other personal details in patron databases.

Consider this scenario: John Public does the recommended steps to protect himself. He doesn't write down passwords; he shreds correspondence that may have privacy information; he locks his mailbox, etc., yet his bank account is accessed and used to fund a wild weekend in Las Vegas. He starts investigating where the leak could be and finds out that someone hacked his local library's computer system. He doesn't think much of this at first—after all, it's *only the library*—until he remembers that the last time he checked out a book, he didn't have his library card, and the circulation clerk used his driver's license to verify his identity.

His driver's license number just happens to be the PIN that he used for his online banking service, which allowed the thieves to transfer money to another account, which, in turn, funded the trip to Vegas. It's the identity theft house of cards "that Jack built."

How did this happen? It happened because the library's network and Integrated Library System (ILS) were not properly secured from illicit access.

Pre-Internet library networks were simple arrangements of hosts and terminals—a closed network providing limited access. Retrieving personal information from an ILS required physical access. Then, the Internet Age arrived. Gone was the need to sit at a library terminal to access the ILS. Library vendors, seeing cost benefits in embracing Internet communication, began making their systems accessible online. These networks were laid out in what is termed a "flat topology." All computers were easily accessible to each other, with few (if any) security limits to communication with the ILS server. There were plain text packets moving to and fro, readable to anyone willing to take the time to grab them. Segmented networks, host security, firewalls, and VPNs were not a part of the equation for accessibility of information.

Through the last several years, we've gained wisdom. Libraries began utilizing firewalls and started working to protect their networks. Unfortunately, communication between the ILS and the client computer is still largely unencrypted.

In the not-too-distant future, we will see an epiphany by identity thieves. They will realize that the insufficiently secured wireless access point in the library is on the same network as the library's

circulation computers. With a network sniffer, they will be amazed at the information, going back and forth in plain text that they can access. They may see useful information such as SSNs and driver's license numbers, as well as names, addresses, email addresses, phone numbers, and passwords used to place holds via the Web site. There's a good chance, being the lazy humans we are, that this password might also work with a bank's Web-based banking system. It won't take long to extract useful information from the data stream. They might even learn enough about the system to log directly into the ILS.

Since this information will concern people in the same geographic area as the thieves, targeted postal theft or email phishing to flesh out additional information needed to apply for credit cards and loans may occur. The thieves will be equipped with all the knowledge they need to commit identity theft against our patrons.

How are libraries to deal with this problem?

The first step is for libraries to start realizing the What, When, Where, and Why of the personal information they store. Libraries need to conduct privacy audits of all systems that access or store personal information concerning patrons—and the ILS is not the only place this information is stored. Pay close attention to other systems, like computer reservation systems and theft prevention systems, as well as any organizations providing patron information (debt collection agencies, etc.) Libraries need to know exactly what information is available, where it is contained, and how/why it is accessed. Librarians have agonized for years over the privacy concerns of retaining circulation transactions. However, we have not made a concerted effort to remove information that we don't need. Even if a library has made a decision to stop requiring information such as SSNs, it probably hasn't taken the additional step of sanitizing the information already stored. This is why we must complement our normal fiscal audits with privacy auditing.

The next step is to require our vendors to make protecting patron privacy an important feature in an ILS. Weak passwords, unencrypted communications, and poor security postures can no longer be tolerated.

How many libraries are still using vendor-delivered passwords on their ILS? Shouldn't that be the first thing you change when the new system is turned over to your library? Circulation software needs to use some form of encryption when communicating with a server. It would not be overly difficult for vendors to build SSL encryption into their software to prevent illegal snooping. Web-based OPACs need strict limits on what patron information can display, along with data verification measures to limit the information they can accept.

A minimum standard for ILS security supported by all vendors is the best place to start. Ideally, this would be independently tested and verified, with all vendors receiving a logo to identify their certified products once they pass the procedure.

The best thing that we can do to ensure this happens is to use our purchasing procedures to stress that protecting patron privacy is a high priority. At the minimum, we need to ensure that patron data is accessed via encryption, and then only when there is a real need. We must control access to our systems, and only share information with systems that we trust. Finally, we need to take measures to limit the effects that less-secure systems can have on our data.

As a postscript to this article, the summer 2005 issue of 2600: The Hacker Quarterly *has a submission detailing how to pull private information from the administrative web module of a library's computer reservation system. The system has since been secured, but the incident should have been avoided by controlling the IP addresses allowing access to the Web page.*

Reach Erik with questions or comments at:
erik.lewis@mac.com

KEN ROBERTS

Chief Librarian,
Hamilton Public Library

Ken Roberts is the Chief Librarian of the Hamilton Public Library. HPL is one of the largest library systems in Canada, with a mixture of urban and rural components. Ken is a co-director, with the City of Hamilton's IT Director, of their community portal project. Ken is a former Children's Librarian who writes children's novels as a hobby. One novel was nominated for the Governor General's Award in Canada and his latest, *The Thumb in the Box*, received a starred review in *The Horn Book*.

I am an administrator. When I think about any issue, including network security, I tend to think about policies and purposes, not the specifications of any technology that might be involved. A quick glance at an issue that has kept most administrators up late at night and consumed entire landfills of paper is instructive.

Internet filtering has been introduced at many library systems in response to a belief by much of the public, many staff, and some IT specialists that filtering would stop inappropriate use at public computers. Filtering may or may not have achieved that goal. Filtering did provide some library staff members and some library costumers with a sense that they were now secure.

Along came wireless technology. Now, people can bring their own laptops to libraries and they can connect to the Internet using their own providers. Technically, they can display any unfiltered images they wish. Technology did not provide a solution to the display of unwanted images inside library buildings. At best it has provided a short breather. The only way to stop such behavior is to provide reasonable expectations of acceptable conduct inside our facilities and then to train staff so that they can enforce these expectations. Technology alone rarely solves problems.

While nobody can realistically predict the security and network issues that libraries will face, I can confidently predict that technology alone will not solve security issues. Effective responses to security issues will involve the use of policies and will involve staff awareness and training.

Here are some obvious challenges we will face.

1. There will be many more access points into our crucial systems. Each time we enable an online capability, we create vulnerability. The Hamilton Public Library now uses an online library card registration system. It is good service and we need to offer it so that residents who discover our online resources can register and use them easily. The system is set up so that there is no direct link to the active patron database, but there is a two-step link that did not previously exist. This service and any new electronic services rely on the diligence of staff to ensure that any handshakes are tepid at best.

2. We are all using an increasing number of vendors to supply our complex array of services. Our servers and network connections and software applications all link together, creating gaps that reduce security. As well, venders A and B might be committed to supplying regular patches and fixes, but vendor C might not supply such upgrades and, indeed, the changes made by vendors A and B might affect vendor C's product

environment. This is a real concern. At Hamilton, we are trying to close a window of vulnerability unintentionally created by the city and library's joint introduction of a community portal.

3. There will be many more ways (e.g. USB drives) that people using library computers can add their own software. They can even copy information from our computers and analyze it at home, looking for network vulnerabilities.

4. There are a number of innocent staff activities that can and will cause us harm:

- More and more staff can request at least some form of deep access into software applications, access that may compromise the software itself if used improperly.
- Staff increasingly bring "drive-by" problems into our systems, unintentionally accepting dangerous streams from sites they might have visited.
- Staff want to place unique software onto work computers, creating support issues when their machines slow down or react to system settings required for key functions.

The solution to each of these issues is an increased emphasis on clear policies and on training, clearly outlining the impact of well-meaning misuse of computers.

I once swore never to predict the future until I was five years from retirement, knowing that any prediction was likely to look stupid within a brief period of time. This is a personal rule I have only once broken. Ten years ago I predicted that no matter what computing advances might be made, the provision of printing services would continue to be a nightmare. I may be shy about issuing predictions, but my track record is good.

Reach Ken with questions or comments at:
kroberts@hpl.ca

upstream

Unexpected Ideas, Uncensored Opinions

SirsiDynix institute

grow your skills