# User Level Security Management in a Library Network

By

Mukut Sarmah

*Librarian*

*Pandu College*

*Guwahati – 781 012*

*Assam*

**E-mail:** sarmah_mukut@rediffmail.com

## ABSTRACT

The primary goal of a library is to provide access to information resources to the users. However, as libraries move from paper to electronic medium, providing access to resources over a network safety has become very complicated. Security of assets or resources in a library network should be achieved without any compromise. But, if users are not protected from easy and unauthorized access to the library network the stored information may be at risk. So, the network must be protected by creating some security policies. Libraries will be able to protect their resources by making sure that users will use only those resources for which they have been granted access. The paper describes how to assist the library network professionals in the process of users' security management.

**KEYWORDS:** Network Security, Access Control, User Identification, Authorization

## 0. INTRODUCTION

Building a secured computerized Library Network is more important and more complicated than ever before. The network administrator must protect the library's networks and systems, and make the resources accessible to the library users. It takes a large-scale, multi-faceted effort to manage the library network security, and it will involve everyone like, library professionals, network administrators, information system personnel, staff etc.

Library network security principles involve creating a multi-tiered security system like, user security, workstation security, server security and network security. Out of these user security is one of the important aspects in a library network, which should be taken into consideration. This is true that we'll never be able to *completely* protect our library network — we can only slow down the attacks.

## 1. GOALS OF A GOOD SECURITY SYSTEM

There are three primary goals of a good security system:

- to protect confidentiality by ensuring private information is kept private.
- to ensure data integrity by preventing data from being inappropriately changed or deleted.
- to ensure data availability by making sure services are available and uninterrupted, that data can be accessed whenever it is needed, and that data can be restored quickly.

Libraries will be able to protect their resources by making sure that users will only use computers, applications, files, data, printing or other services for which they have been granted access. Users will not be able to login to databases without meeting the Library's access requirements.

## 2. LIBRARY SECURITY PRINCIPLES & POLICIES

Securing any computer in a library network must be achieved without any compromise. Security is a matter of making sure that documents and transactions haven't been tampered with, confidential information is protected, and required information is made available when the user wants it. Computers of the library networks must be available and able to withstand long hours of uninterrupted use. This means it is up to network administrators to ensure data integrity and availability. Online Public Access Catalogue (OPAC) should be made available whenever users want to access the catalogue. Users should not be frustrated due to poor implementation of a security policy. Otherwise, the user's perception on the library may be negatively affected. Library staff and information systems personnel should work together to complete two very important tasks for obtaining a secured library network:

- Perform a Risk Assessment, which should include threats and vulnerabilities facing the library's

computers and networks.

- Create a Security Policy, which includes specific protection strategies.

## 2.1 Risk Assessment

Risk Assessment is a process that helps libraries to become more aware of what do they posses and what is most important to them. Risk is the possibility that someone or something will either intentionally or unintentionally exploit or attack a computer or system, resulting in damage to that asset. An asset is something of value to our library. It can be: information and intellectual property, computer hardware, computer software etc. Examples of information and intellectual property assets include: the library's original bibliographic database; CD-ROM databases; locally created Web sites; staff e-mail; library procedures and policies; staff documents; circulation data; financial records and so on.

Risk can never be eliminated completely; it can only be reduced to an acceptable level. That level will vary according to the importance of an asset to a library. A Risk Assessment will help a library better understand their risks by weighing the likelihood that an asset will be attacked versus its value versus the cost of protecting it.

## 2.2 Creating a Security Policy

Security policies are not easy to create. A Security Policy can be one policy or a collection of policies that state what the library should protect, how it should be protected, how to respond to security threats, and who should be involved in that response. Furthermore, they must be constantly reviewed and updated in response to changes in the organization, additional hardware or software, new vulnerabilities, and new threats. Compliance is another activity that includes details about the actions to be imposed if the security policy is violated. This may include: disconnection from network, loss of network privileges, personnel disciplinary action, legal action.

# 3. COMMON THREATS AND VULNERABILITIES

Threats to computers and networks have been an issue since computers began to be used widely by the general public. Nowadays, any computer or library network connected to the Internet is at risk. Basic types of attacks include:

· **Probes and scans -** attempts to gain access or discover information about remote computers

· **Account compromise -** discovery of user accounts and their passwords

· **Packet sniffing -** capturing data that is sent across a network; the data can contain sensitive information like passwords

· **Malicious code -** Worms, viruses

Although there are various vulnerabilities in computer systems and networks today, the main vulnerabilities that are likely to cause us harm are: default software installations, ineffective use of authentication, backups not maintained and verified, lack of protection against malicious code.

## 4. USER LEVEL SECURITY: STRATEGIES

Protection strategies are the specific techniques that the security team will use and the procedures they will follow. Providing access to information resources is a primary goal of libraries. However, as libraries move from paper to electronic medium, safely providing access to resources has become complicated. Making public access workstations available to the users in a library network can also develop unauthorized access to resources and cause damage or loss of data. Therefore, security-conscious network administrators must secure and control access to library resources. This is done through a process called "access control."

### 4.1 Access Control: When to Use

Controlling access to resources depending on who wants to access them is called "user-level security." This kind of security can be used to regulate access to networked or stand-alone systems. There are various reasons to implement user-level security in a library network, which are:

· There are resources on our network for both library staff and users; however, users should have access only to specific, limited resources.

· A library needs to provide unfiltered Internet access to staff but only filtered Internet access to its users.

· It is important to understand that user-level security and ease of access are inversely related: the more security required to protect a resource, the more difficult it becomes for users to access that resource.

### 4.2 Access Control: Steps

Access control is a three-step process that involves **identification, authentication,** and **authorization**.

**4.2.1 User Identification:** Before accessing a resource, a user must first identify him or herself. User identification is the process of establishing the user's identity and usually requires very little interaction on the user's part. Once a user has identified himself or herself, a system can check whether that person has previously registered and is in fact allowed to use the system. There are two popular methods of user identification in libraries. Library cards with magnetic strips or bar codes allow patrons to carry their identification with them in a physical form. The other popular method of identification is a username. This method requires the user to remember their identification; this is used primarily when logging in to a computer.

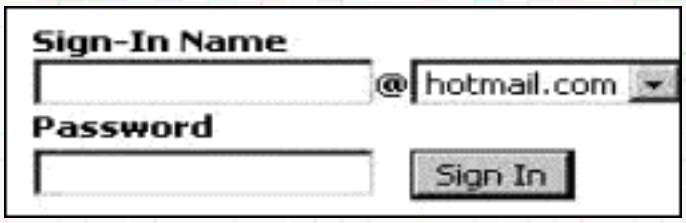
Obtaining a library card is the most common way of registering an identity. Once a user's or staff's identity is registered, the library can then determine what resources that user can access. Registration can require a lot of administrative overhead. A common practice is to register a generic user account that is available to all users. This practice is beneficial when a user is accessing a resource that is not sensitive. In this case, all users have the same identity and authentication is avoided.

**4.2.2 Authentication:** Authentication is the process of proving a person himself or herself as an authorized user. The goal of an authentication system is to verify who a user is? what data is available to that user? A user can be authenticated because of:

- something she or he knows (such as a password or PIN)
- something she or he has (such as a library card)
- something she or he is (such as a person with a unique fingerprint or retina)

Strong authentication demands at least two of these methods used together to verify a user. For instance, a user could be authenticated first by their library card (something s/he has) followed by a Password or Personal Identification Number (PIN), (something s/he knows).

The use of passwords is one of the most common forms of authentication. We use passwords for our e-mail, when we login to a network. Unfortunately, passwords can also be one of the more useless forms of authentication if they are not constructed properly. If our password is easy to guess, if we use the same password (our middle name) for every account you have, or we leave our password blank, then we are simply making it that much easier for hackers to access our accounts.




The shorter the password the easier the hacker's task becomes. Furthermore, the longer someone has a password, the more likely it will be that he or she will tell someone else what it is, or that they will be able to guess it. Passwords that are not easily guessed are called "strong" passwords. A strong password is one that uses a random mixture of letters, numbers, and characters. The goal of a strong password is to slow attackers down. Our library or information centre should consider adopting some rules for network passwords: passwords may not be blank; passwords must be seven or more characters long; passwords must use a mixture of letters (upper and lower case), numbers and characters; passwords must be changed on a regular basis; passwords must be successively unique (in other words, users shouldn't use the same password repeatedly); passwords must never be written down or posted in an insecure location (such as on a monitor).

In addition, we can consider adding these prohibitions: passwords cannot be the user's name, the name of someone in their family, or their birth date; passwords must not be constructed by adding a numeral or character to the beginning or end of a regular word, this is too easily guessed (e.g."sarmah1"). We should give our users tips on how to construct strong passwords.

Each of these authentication methods has drawbacks. Password or PIN authentication is easy and inexpensive, but it requires that the user commit something to memory (which is often easy to forget). Passwords can also be susceptible to compromise, depending on their length and what kinds of characters are used.

Library cards can store and track a lot of useful information, but unless they are password protected, a stolen card can be easily compromised. Card readers are more costly than password and PIN authentication.

Biometrics literally means "life measure." It is a method for automatically identifying users based upon their unique physical characteristics, such as their retinal pattern or their fingerprints. They are useful for providing security for sensitive data. It is very hard to compromise this kind of security. However, biometrics can be highly cost prohibitive. Retinal scanners are still somewhat of an emerging technology, but fingerprint scanners are available now and cost less than retinal scanners.

**4.2.3. Authorization:** Authorization is the final process in user-level security. It is the process of

determining what resources a user can access after successful identification and authentication.

Different users have different authorization to library resources. For example, a user should only have authorization to read from a card catalogue system, but a staff user should have authorization to make changes or modifications to records in the system, and an administrator should have full control to change anything—including what kind of authorization other users have. Another example is Internet filtering. Administrators and staff should have unlimited access to the Internet; however, patrons should only be authorized to view filtered content.

It is up to the library automation staff to implement authorization. However, when implementing network security great care should be taken in determining what resources users are authorized to access. Security is as strong as the weakest link. If a system has a strong identification and authentication process but a weak authorization process, security may be easily compromised.

## 5. CONCLUSION

Library networks are created to make provision for accessing the resources by the users from remote computer systems. At the same time there is a risk or possibility that someone or something will intentionally or unintentionally attack a computer system, resulting to damage to the resources. The resources or assets in a library network must be protected form these attacks following security policies and principles. Controlling access to the resources involves three basic steps like, identification, authentication and authorization. It is true that we can never completely protect our library network from the unauthorized users but the attacks can be minimized up to a desired level.

## WEBSITES VISITED

1) http://www.faqs.org/rfcs/rfc2504.html

2) http://www.infopeople.org/howto/security/users/passwords.html

3) http://www.ietf.org/rfc/rfc2196.txt

4) http://www.sans.org/newlook.resources/policies/policies.htm

5) http://www.csrc.nist.gov/publications/nistpubs/800-18/planguide.pdf

6) http://www.zonelabs.com/

7) http://www.symantec.com/sabu/nis/npf

8) http://www.mcafee.com/myapps/firewall/default.asp

9) http://www.microsoft.com/security

10) http://www.microsoft.com/technet/security/bulletin/notify.asp

11) http://home.netscape.com/security/notes/

12) http://www.netscape.com/download/

13) http://www.microsoft.com/windows/ie/default.asp

14) http://www.microsoft.com/windows/ie/support/default.asp

## BRIEF BIOGRAPHY OF AUTHOR

***Mukut Sarmah*** is the Librarian, Pandu College, Pandu, Guwahati. He holds B. Sc. in Botany, B.L.I.Sc. and M.L.I.Sc from Gauhati University, Guwahati. He is registered for Ph.D. in Gauhati University. He also worked at DLIS, Gauhati University and IIT-Guwahati