Dibentangkan Di
Seminar Kebangsaan Teknologi Maklumat Di Perpustakaan
Anjuran Perpustakaan Sultanah Bahiyah, Universiti Utara Malaysia

Sesi 4 : Pengurusan Rangkaian dan Sekuriti
4 Ogos 2010 | 2.30 – 5.00 petang | Bayview Hotel, Pulau Pinang

SECURING LIBRARY INFORMATION SYSTEM: VULNERABILITIES AND THREATS

Oleh / By

Hatim Mohamad Tahir
Nurnasran Puteh
Mohd Zabidin Hussein
College of Arts and Sciences, FTM Building, Universiti Utara Malaysia
06010 UUM Sintok, Kedah, MALAYSIA
{hatim@uum.edu.my ; nasran@uum.edu.my }

Abas Md Said
Computer and Information Sc Dept, Universiti Teknologi Petronas,
31750 Tronoh, Perak, MALAYSIA
abass@petronas.com.my

(Presented at National Seminar On Information Technology In The Library at Bayview Hotel, Penang, Malaysia : Session 4 – Networking and Security Management, 4th August 2010 2.30 – 5.00 p.m. Seminar organized by Sultanah Bahiyah Library, Northern University of Malaysia : http://www.lib.uum.edu.my)

SECURING LIBRARY INFORMATION SYSTEM: VULNERABILITIES AND THREATS

Abstract:

Threats and vulnerabilities in computers and networks are common nowadays since computers are widely used by the public. The risks of computer threats and vulnerabilities are high since most computers are connected to the internet. Library Information Systems is also vulnerable to attack since it is a public access institution. Majority of users are naive when it comes to computer and network securities. Some breaches in Library Information System are intentional and some are unintentional. Risks analysis should be done to find the threats and risks in designing the Library Information System. Threats are made possible due to lack of proper procedures, software flaws and policies. The administrators should anticipate all the possible attacks and their mitigation techniques. In this paper, we will try to address various issues arise from this vulnerabilities and threats. We will also describe how we can reduce and overcome this vulnerabilities and threats.

I INTRODUCTION

The advanced of internet in today world, open the opportunities for people to connect and be connected. Internet has dramatically change how people communicate, conduct business and interact with each other. As internet has make life 'easier' so is the threats posed by internet. Threats to computers and networks have been an issue and still haunting internet users. Nowadays, any computer or network that is connected to the Internet is at risk. CERT (the Computer Emergency Response Team funded by Carnegie Mellon University) cautions that *"intruders form groups and develop scripts that they share with each other on how to maliciously exploit vulnerabilities in systems. Intruders dedicate time to developing programs that exploit vulnerabilities and to sharing information. They have their own publications, and they regularly hold conferences that deal specifically with tools and techniques for defeating security measures in networked computer systems."*

Library as a public institution is accessible from anywhere are posed to numbers of threats and breaches. A library computer system security is bound to be attacked if no specific precautions are taken. The magic word 'prevention is better than cure' is applicable in the computer and network security. Many big incidents affecting computer and network security can be read from Malaysia CyberSecurity (www.CyberSecurity.my) and CERT websites.

II BASIC TYPES OF THREATS

In safeguarding the Library Information System, we need to identify the basic types of attacks that a intruder or hackers will used. The basic type of threats are:

i) Probes and Port Scanning
Relative to computer security in a network, a probe is an attempt to gain access to a computer and its files through a known or probable weak point in the computer system. One example is an attempt to log into an unused or idle account. Probing is the equivalent of testing doorknobs to find an unlocked door to gain entry. Probes are sometimes followed by a more serious security breach. A port scan or port scanner attempts to connect to all 65536 ports on a server to see whether there are services listening (that is, waiting for connections) on those ports. The purpose of a port scan is to audit network computers for likely vulnerabilities or exploits. Typically, scanners have built-in databases of known port vulnerabilities. Scans are often a prelude to a more directed attack on systems that the intruder has found to be vulnerable.

ii) Account Compromise

An account compromise is the unauthorized use of a computer account by someone other than the account owner. It allows an unauthorized user to gain access to all resources for which that user account is authorized. An account compromise might expose the victim to serious data loss, data theft, or theft of services. Limiting the amount of user accounts that have root-level access or administrative privileges minimizes potential damage.

One kind of compromise better known to UNIX systems is called a root compromise. Traditionally, the administrative account for UNIX systems is called root. Not only is it a user name, but it refers to the highest level directory on a server. If an account has root level access, it usually has access to the entire system. Intruders who succeed in a root compromise can do just about anything on the victim's system, including run their own programs, change how the system works, and hide traces of their intrusion.

iii) Packet Sniffing

A Packet Sniffer is a program that can record all network packets that travel past a given network interface, on a given computer, on a network. The data may include such as user names, passwords, and proprietary information that travels over the network. If the data captured by a packet sniffer is encrypted, it is unlikely that someone will be able to reveal any sensitive information. However, if the data is not encrypted, just about any information sent is vulnerable to being compromised. Installing a packet sniffer does not necessarily require privileged access; however, it requires obtaining access to a network card interface somewhere in the line of communication

iv) Denial of Service (DoS)

The goal of denial of service attacks is to prevent legitimate users of a service from using it. A denial of service attack can come in many forms. Attackers may "flood" a network with large volumes of data or deliberately consume a scarce or limited resource such as processes or network connections. They may also disrupt physical components of the network or manipulate data in transit, including encrypted data. The underlying purpose of a denial of service attack is to make the system too exhaustive (slow or stand-still) to process request from users.

v) Malicious Code

Malicious code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. Users of the system usually are unaware of the program until they discover the damage. Malicious code includes Trojan horses, viruses, and worms. Trojan horses and viruses are usually hidden in legitimate programs or files that attackers have altered to do more than what is expected. Worms are self-replicating programs that spread with no human intervention after they are started. Viruses are also self-replicating programs, but they usually require some action on the part of the user to spread inadvertently to other programs or systems. These sorts of programs can lead to serious data loss, downtime, denial of service, and other types of undesirable effects.

vi) Spoofing

Computers on networks often have trust relationships with one another. Spoofing is the practice of deceiving people into believing an email or Web site originates from a source that it does not. The most common type of spoofing is email spoofing, but Web page spoofing and IP spoofing are also very common. If attackers can forge their identity, appearing to be using the trusted computer, they may be able to gain unauthorized access to other computers.

III BASIC TYPES OF VULNERABILITIES

Although there are many vulnerabilities in computer systems and networks today, the main vulnerabilities that are likely to cause you harm are:

i) Default Software Installations

A default software installation is where an operating system or application software is installed using all the default settings built in by the programmers or vendors. Performing a default software installation on computers with sensitive data is not good practice, especially when the chosen software is likely to be used by many people, such as on a public access computer or web server.

Servers are installed with default user accounts. It is therefore important to:

- Disable guest accounts
- Don't run important daemons as root (inetd)
- Rename the administrator account
- Set a strong password for the administrator account

ii) Ineffective Use Of Authentication

Authentication is the process of proving who you are to a system using one or more authentication methods. Authentication can be based on what you know (such as a password), based on what you have (such as a smart card), or based on who you are (such as biometrics). Most organizations rely on authentication via passwords. Passwords can be a fairly secure form of authentication when they are created properly. Users normally try to use passwords such as birth date, car registration number, matrix number which is unadvisable.

iii) Software or System Patches

Software or System patches are needed to patch known security problems due to the nature of software and system updates. As software vendors write increasingly complex code, it becomes harder for them to keep up with making the necessary patches. Server and systems administrators must make the effort to keep their systems patched. For information on where to find system and software patches are always posted on vendors website.

iv) Too Many Open Ports And Services Running

Ports are labels—ways to identify services that are running on particular machines. Ports have identification numbers which are included with every TCP or UDP packet. Services that are running on a machine are programmed to be on the alert to "listen" for packets that arrive from other computers with matching port numbers. Thus, the types of ports your server has open can give away a lot of information about it. In addition, the more ports your servers open, the more options there are to connect to that server.

v) Not Analyzing Incoming Packets

A packet is the smallest unit of information that is transmitted across networks. All information—web pages, email messages, etc.—are broken down into packets before being transmitted. Each packet of a transmission has the service's port number, the sender's IP address, the destination IP address, and a packet number. All of the packets in a transmission are numbered in sequential order. Analyzing incoming packets allows you to filter out packets that don't match the rules that have been built into a network device's such as firewall. It also allows system administrator to watch for unusual activity. Analyzing your network traffic for unacceptable traffic is usually only done when there is a suspected breach of security. Proactively analyzing network traffic as a preemptive function is normally only done on networks with extremely sensitive data.

vi) Backups Not Maintained And Verified

One of the aims of risk assessment is to show how many hours an asset such as a server can be down before it starts to impact the library's mission. If backups are not made daily, or at an interval acceptable to your library, we will not be able to quickly recover from data loss caused by security breaches or other disasters. Backups also should be tested to ensure that data has been backed up properly and that staff has enough familiarity with the recovery procedure.

vii) Lack Of Protection Against Malicious Code

A virus is a program that reproduces by attaching to another program. It may damage data directly, or it may degrade system performance by taking over needed system resources which are then not available to authorized users. Worms are independent programs that reproduce by copying themselves from one system to another, usually over a network. Trojan horses are programs that appear to perform a useful function but actually hide another unauthorized program inside them. When an authorized user performs the apparent function, the Trojan horse performs the unauthorized function as well (often usurping the privileges of the user).

All of these threats and vulnerabilities must be anticipated, especially when the threat is due to staff ignorance. They certainly must not be ignored—an ostrich with its head in the sand is only getting its head dirty. Threats and vulnerabilities must be carefully examined to see whether or not they apply to your library's computers and networks, staff and procedures. Then they must be analyzed to devise strategies to counter them.

IV RISK ASSESSMENT

Risk Assessment is a process that helps organizations become more aware of what they have and what is most important to them. Ideally, it should involve the whole organization which works together to identify all information technology assets, to assign a priority rating to each, and to identify threats and vulnerabilities to these assets.

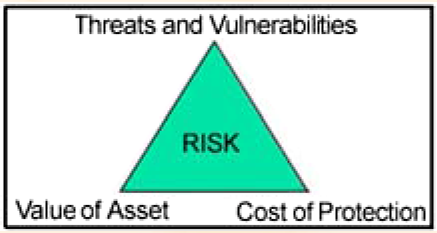


Fig.1.0: Risk Assessment

In practice, a team is usually assembled comprising of IT managers and staffers, library administration personnel, and members of various other departments.

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. Risk can never be completely eliminated; it can only be mitigated and reduced to an acceptable level. The level will vary according to the importance of an asset to an organization. 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.

V. DETERMINING YOUR ASSETS

An asset is something of value to your organization. In information technology terms, it can be:

- Information And Intellectual Property
- Computer Hardware
- Computer Software
- People

Examples of information and intellectual property assets include: the original cataloging in a library's bibliographic database; locally created indexes and databases; locally created websites; staff email; and library procedures and policies. Computer hardware could include all servers, telecommunications equipment, desktop computers, printers, backup devices and cables. Software assets might include desktop operating systems such as Windows 2000 or UNIX; productivity applications such as office suites; server operating systems; and server software. Finally, human assets should never be overlooked. They might include administrators, IT staff, catalogers, reference staff, technical services staff and so on.

Once a list of the library's assets has been created they should be assigned a "threat rating," by evaluating them in terms of their importance to the library's mission.

a) **High** — Your library would suffer major disruption and legal or financial loss if the asset is attacked. Without this critical asset, your library would be sufficiently damaged as to no longer be able to fulfill its mission.
b) **Medium** — Your library would suffer minor disruption and legal or financial loss if the asset is attacked. Without this important asset, the library would still be able to fulfill its mission, but in a limited capacity.
c) **Low** — Your library would suffer no disruption, legal or financial loss if the asset is attacked. Your library would be able to completely fulfill its mission without this trivial asset.

Computer assets are constantly exposed to threats and vulnerabilities. A threat is a situation in which someone or something deliberately compromises confidentiality, integrity or availability. A vulnerability is a flaw in software code which might be exploited to perform attacks on the networks or computers which use that software. Listing the threats and vulnerabilities of a library's computers and networks is a vital part of a Risk Assessment.

Finally, it is important that once the Risk Assessment is complete it be put to use. Now that your organization has a clearer idea of what assets it is protecting, it should make decisions on how to protect them. The Risk Assessment merely answers the questions what and why.

VI. CREATING A SECURITY POLICY

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.

Creating a Security Policy involves several preliminary steps:
a) Create a security team
b) Develop usage policy statements
c) Review security policies from other similar organizations
d) Conduct a risk assessment

A security team should be the group that not only creates the policy but also is responsible for its implementation. Team members should include library administration staff, librarians who are responsible for systems and computers, IT staff who are responsible for systems and computers, and staff who assist with the public use computers. Ideally, a representative from each department will be included.

There are two broad categories of usage policy statements: statements of the library's roles and responsibilities and statements concerning users' roles and responsibilities. Some of these statements may be pre-existing, such as a Remote Access Policy, a Password Policy and an Acceptable Use Policy. These can simply be reviewed (and updated if necessary). A Library Security Roles and Responsibilities Policy should state what the library does to protect and maintain resources and why. For instance, the policy could state that the library provides desktop security measures, anti-virus software, Internet filtering (or not), and so on. Reasons for these measures should be explained.

Users' roles and responsibilities policies are more numerous. They may include statements such as:

a) What is acceptable on the library's network, including staff and public access computers
b) Computers and network are owned by the library, and that they are:

- Provided for the public for specific reasons
- Provided to the staff for specific reasons

c) Which local statutes and federal laws, end users must follow when using library network including:

- Laws governing use of copyrighted materials
- Laws governing obscenity and child pornography

d) What is NOT allowed:

- Using email to harass or intimate anyone
- Running password crackers
- Installing unlicensed or pirated software
- Turning on file-sharing
- Running streaming media applications

e) Whether or not system is monitored
f) How the library enforces the policy; what happens if someone is caught breaking the rules
Whenever possible, review security policies from other similar organizations—after all, why re-invent the wheel? Most universities have security policies available online. Finally, conduct a Risk Assessment to determine what assets the library wants to protect and why. You may want to include this as part of the security policy effort.

VII. COMPONENTS OF A SECURITY POLICY

A Security Policy has the following basic components:

a) Objective
b) Scope
c) Responsibilities
d) Physical Security
e) Network Security
f) Software Security
g) Disaster Contingency Plan
h) Acceptable Use Policy
i) Security Awareness
j) Compliance

The Objective should be a mission statement that defines objectives of the policy. It summarizes what types of assets are important, why the library needs to protect them, and summarizes procedures to be followed to protect assets. The Scope defines the specific assets to be protected by the policy, based on the Risk Assessment. It also defines who must follow the policy, such as members of the public, employees, outside contractors, and vendors. The Responsibilities components describes who is responsible for protecting assets defined in the scope, and how. It generally outlines users' security responsibilities, but it can also include roles of particular users, such as IT department managers and administrators.

The Physical Security section states how the library will physically protect its facility and assets. It should also state who has access to restricted areas, such as server rooms and telecommunications closets. Network Security states how the library will protect data stored on the network(s). It should include information on:

i. Workstation security
ii. Access control and authentication measures
iii. File system security
iv. Backups
v. Remote access controls
vi. Network monitoring
vii. Port restrictions
viii. Filtering
ix. Firewalls, proxy servers and border routers

Software security states how the library will use commercial and noncommercial software on servers, network devices and workstations. It describes who is allowed to purchase and install software, who can download from the Internet and how to deal with violators. The Disaster Contingency Plan should cover both hardware and software. The section on hardware should include a list of equipment to be saved; a detailed hardware inventory with hardware specifications needed for critical assets; a list of the personnel needed to restore servers; and a restore priority. The software section should include information on the software/data backups, off-site storage locations, backup information, personnel needed to restore data, and a restore priority.

An Acceptable Use Policy details the acceptable ways in which the network can be used, including acceptable use of the Internet, acceptable use of computers, limitations on computer use (such as time constraints or filtering restrictions), and sanctions to be imposed if acceptable use standards are not met. Security Awareness states what level of awareness of security issues staff are expected to have. Compliance includes details about sanctions to be imposed if the security policy is violated. Sanctions may include:

i. Disconnection from network
ii. Loss of network privileges
iii. Personnel disciplinary action
iv. Legal action

Security Policies are not easy to create. They require a lot of effort by many people. Furthermore, they must be constantly reviewed and updated in response to changes in the organization, additional hardware or software, security breaches, new vulnerabilities, and new threats.

VIII. PROTECTION STRATEGIES

Critical to your library's Security Policy are your protection strategies. These are the specific techniques your security team will use and the procedures they will follow to ensure the outcomes spelled out in the Security Policy. They should include the following strategies:

i. Never assume a default software installation is secure
ii. Always require strong authentication
iii. Always perform and verify backups
iv. Close all unused ports
v. Protect your network boundary
vi. Use anti-virus software
vii. Use desktop security software
viii. Always monitor logs
ix. Keep software patched

i) Never Assume a Default Software Installation Is Secure

Software vendors make their installation programs as generic as possible, focusing on ease of use rather than good security practices. There are four separate vulnerabilities you should be aware of when installing an operating system or application.
a) Default services installed (mainly applies to operating systems;, you should always check what services are installed with applications as well)
b) Flaws in code
c) Sample scripts and templates
d) Default accounts and passwords

ii) Default Services

Most operating system installation programs and even applications will install a fair number of services by default. A service in the Windows family of operating systems is software that, once started, runs without interaction from users and performs a variety of tasks, from maintaining network communications to managing printers to performing URL and IP address translations.

Services are sometimes designed to open certain channels of communication called ports. Once a service that opens a port is installed and started, it maintains an open window of communication and waits to be contacted. It also uses memory and processor resources. Leaving port open allows an unnecessary open window through which someone can possibly exploit vulnerabilities in the service. In order to mitigate against this vulnerability in operating systems, always be sure to uninstall (or, better yet, never install in the first place) unneeded services. Doing this will save memory and processor resources, as well as secure the computer.

iii) Flaws in Code

Another problem with installing any software or operating system is related to the fact that they are, by nature, complex. By the time software is released to the general public (perhaps prematurely because of market pressures), it inevitably has flaws. These flaws are called bugs. The only solution is to always be sure to immediately install patches or service packs for the operating system or application after their installation.

iv) Sample Scripts and Templates

A third problem is that vendors sometimes include sample scripts and templates to help the end user with common administrative functions. The most commonly known sample scripts are those provided with a default installation of Microsoft's Internet services. Because everyone knows what these samples do and exactly where they are installed, hackers can exploit these sample scripts and do anything from causing damage on a computer to gaining full control of the computer. Always uninstall sample scripts, databases, etc. before releasing an application or operating system into production.

v) Default Accounts and Passwords

Finally, in the interest of making a product easy to use, vendors often set up generic user accounts and passwords as part of a default installation. Like sample scripts and templates, operating systems often provide generic accounts and passwords by default. Unless you change the defaults, an attacker will find it relatively easy to hack into a server simply by logging in as a user with the generic password! To protect against this all too easy attack, always change the administrative account password. Microsoft always forces you to create a unique administrative password; however, a guest account is often created that uses no password. In addition, consider renaming the account. If a hacker doesn't know what the account names are, s/he won't be able to perform a "brute force" attack by trying all possible password combinations for a particular user. Disable guest accounts whenever possible and if using a Windows operating system, restrict the "Everyone" account on as many directories as you can.

vi) Always Require Strong Authentication

The goal of an authentication system is to verify who a user is, which then determines what data is available to that user. A user can be authenticated because of something she or he knows (such as a password), something she or he has (such as a smart card) or something she or he is (such as a person with a unique fingerprint or retina).
It is important to educate users about how to create a good password, because weak ones can be fairly easy to figure out with the right tools and knowledge. As soon as a password is compromised, especially one that belongs to a user with administrative access or extensive rights, the entire security system falls apart.

vii) Always Perform and Verify Backups

In an emergency where one or more of your servers has gone down and must be restored, having reliable backups of your data is critical, especially if you can't afford to be down for very long. If backups are not made daily or at an interval acceptable to your library, you will not be able to quickly recover (or recover at all) from data loss. You should create backup procedures that state what data must be backed up, when backups must be made, how they must be tested, where the backup media is stored, and how restores are performed.

It is important to establish an off-site storage location for backup media. When determining an off-site storage location, it is important to consider ease and frequency of delivery of backup media, safety from fire and other disasters specific to the area, and security depending on how sensitive the data is. It may also be a good idea to maintain a set of installation media for the backup software as well as some kind of backup hardware, should the production environment fail. This way, it is possible to at least restore data and access it. Test the integrity of your backups, as well. An easy method is to back up and restore a test file. Try to also test databases, websites, com objects and other features that may need further configuration beyond just a simple file restore.

viii) Close All Unused Ports

As described above (Windows Services), ports are open windows to a computer that wait for a particular kind of communication. Ports have identification numbers which are included with every TCP or UDP packet. Services that are running on a machine are programmed to be on the alert to "listen" for packets that arrive from other computers that have the same port number as they do.

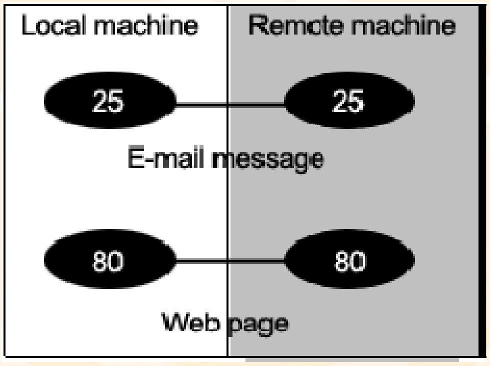


Fig. 2.0: Ports Connection

The more ports your servers have open, the easier it is for attackers to connect to that server. Just as bad, the types of ports your server has open can give away a lot of information about it. One of the first things a hacker will do is monitor your network traffic to try to see which ports are in use. An important security implementation is to restrict what traffic is allowed into your network by only allowing traffic through certain ports on your firewall.

Periodically scan computers on your network to see what ports are open. This gives you a clearer idea of what open ports and traffic exist on your network, and over time it should enable you to spot attacks because you will notice additional ports open that were once closed. The best way to do this is to run a port scan on each individual server, and then run a network-wide port scan. Then you should compare the two lists. If they differ you should find out why and close any ports that have no reason to be open.

ix) Protect Your Network Boundary

The boundary between your library's network and the Internet (or the rest of your organization if you use their Internet connection) is an important one. It is one of the most vulnerable points in your network because it is the point through which all incoming and outgoing traffic must pass. It is therefore extremely important to protect it with some sort of device such as a firewall (or at the very least a router with access lists) that looks at network traffic in two ways: traffic that originates on the inside, and traffic that originates on the outside. Thus a boundary is created; it establishes what is acceptable incoming and outgoing traffic and what should be turned away.

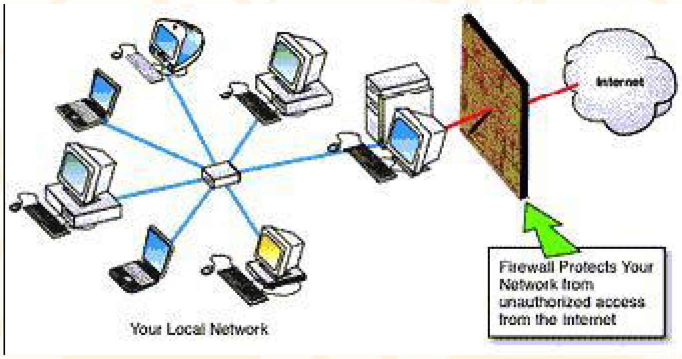

Internet
Firewall Protects Your Network from unauthorized access from the Internet
Your Local Network

Fig. 3.0: Network Boundary

If you have servers that need to be accessed from the outside, such as a bibliographic database server, a web server or an email server, consider establishing a perimeter network (also called a DMZ) that allows these servers to be accessed while still protecting the rest of your network.

x) Use Anti-Virus Software

Using anti-virus software is a necessity nowadays. Back in the days when viruses primarily spread through infected floppy disks, a library could get away with disabling floppy drives and be done with it. With the advent of the Internet-borne virus, those days are over. Viruses and worms now spread with terrible swiftness and can cause amazing damage. The Code Red virus infected over 250,000 systems in 9 hours on July 19, 2001 and NIMDA and Code Red worms cost business 3-6 billion dollars.

Not only must anti-virus software be installed on all servers and workstations, virus definition files must be constantly updated. If your library is large enough, consider purchasing anti-virus software that has a management component that allows automatic DAT updates and virus scans over the network.

xi) Use Desktop Security Software

The security features that come with operating systems are sometimes not enough to meet the needs of a library. This is especially true with public access workstations. For that reason, desktop security software should be added when the operating system cannot provide enough security.

Certain operating systems are less vulnerable than others and may have less of a need for desktop security software. For instance, Microsoft has taken great pains to add many new security features to its newer operating systems Windows 2000 and Windows 7. For those library public access computer administrators who still use Windows 95 or Windows 98, using desktop lockdown software is strongly advised.

xii) Always Monitor Logs

Keeping a close eye on a server's logs is one of the best ways to know when your network is under attack. Logs can show what ports are being opened, what files are being accessed, and what services are being run. Even more important, logs can show when someone has tried to log in with an incorrect password or access a resource. If your server or network is attacked, your log files are a good place to start investigating. Archive your logs on a regular basis so that the log files cannot be overwritten or erased by attackers who want to cover their tracks. If possible, configure your logs to automatically alert an IT staffer if an attack is detected, either by sending an email or generating a page.

xiii) Keep Software Patched

Finally, all software must be kept patched. As mentioned above, software code is complex.Iit is a given that once a new operating system is released, it will have bugs. In fact, there is a vulnerability life cycle:

i) Software release
ii) Vulnerabilities discovered
iii) Vulnerabilities published
iv) Patches released
v) Software hardened
vi) New vulnerability discovered

Server and network administrators must constantly be on the alert for software vulnerabilities, and they must evaluate and install patches as soon as they are released. However, not all patches are necessary; administrators must first be sure that their systems need the patches. Also, some patches can cause more trouble than they are worth. If possible, test patches on a minor system before installing on critical servers. In order to keep up with bugs and vulnerabilities, check the web pages of your software vendors for postings.

IX. CONCLUSION

All Library Information System (LIS) should be maximally secured. Good security practices and policies should be adversely followed. Librarian should always have in their hindsight that hackers and intruders will alway try to attack the LIS at anytime and from anywhere. Maximum protection and well-trained staffs are needed to handle any security incidents.

Acknowledgement:
Part of the materials in this paper is source from various Internet sources with modification and elaboration to suit the topic.

REFERENCES

Security In Computing, Charles P. Pfleeger, Prentice Hall, 4th Ed, 2007

Dieter Goldman, Computer Security, John Wiley 2006

Network Security Essentials – Applications and Standards, William Stalling, 2nd Edition, Prentice Hall, 2003.

Computer Security: Art and Science, Matt Bishop Addison Wesley Professional, 2003

Web Security: A Step-by-Step Reference Guide, Lincoln D. Stein

Information Security and Authenticity on Public Networks. Solutions to some problems raised by conducting private conversations in public places. Rosenthal, C. 2001.

http://www.cybersecurity.my

http://www.ietf.org

http://www.sans.org

http://www.csrc.nist.gov

http://www.webopedia.com/

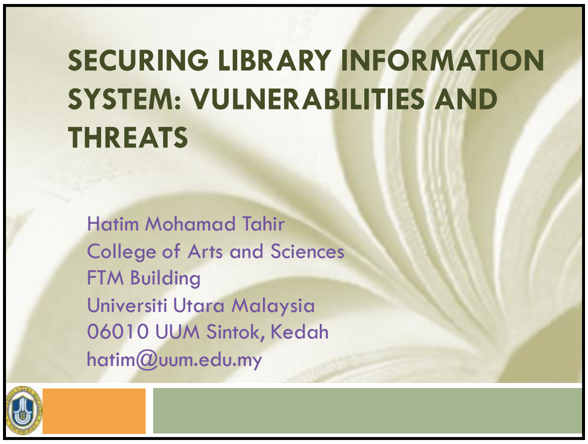
http://www.answers.com

http://www.securitywebsites.com

http://searchsecurity.techtarget.com

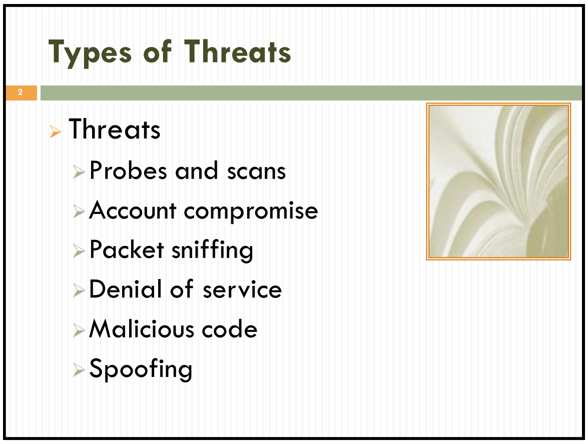
http://www.businessdictionary.com

http://www.us-cert.gov



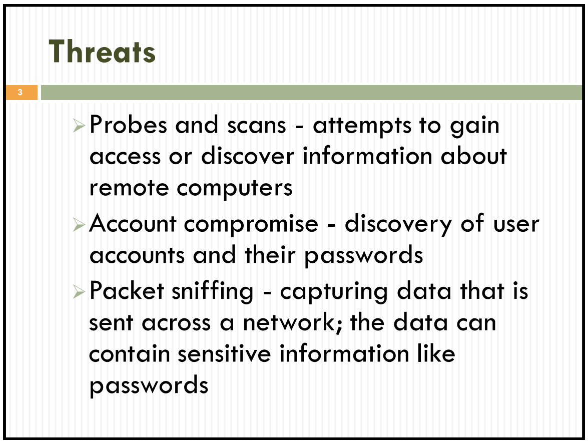
SECURING LIBRARY INFORMATION SYSTEM: VULNERABILITIES AND THREATS

Hatim Mohamad Tahir
College of Arts and Sciences
FTM Building
Universiti Utara Malaysia
06010 UUM Sintok, Kedah
hatim@uum.edu.my



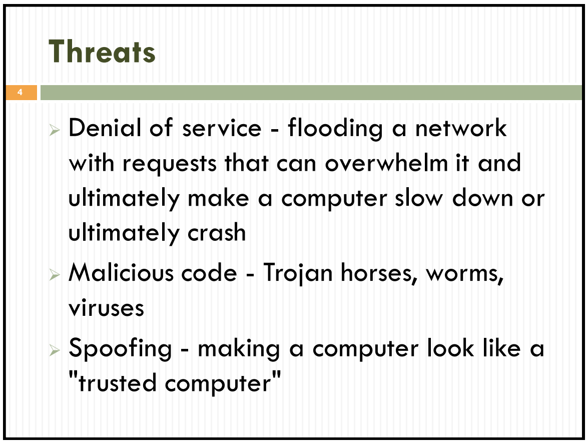
Types of Threats

- Threats
  - Probes and scans
  - Account compromise
  - Packet sniffing
  - Denial of service
  - Malicious code
  - Spoofing



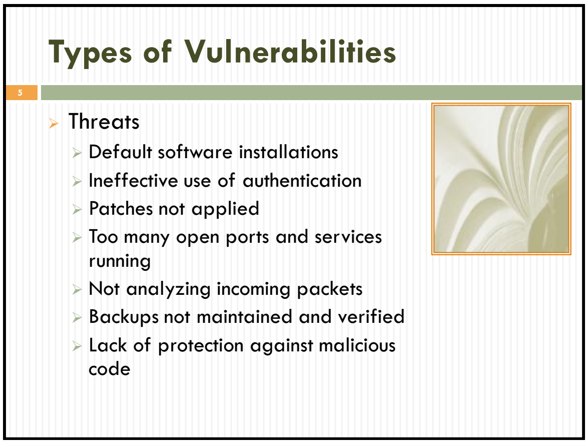
Threats

- 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



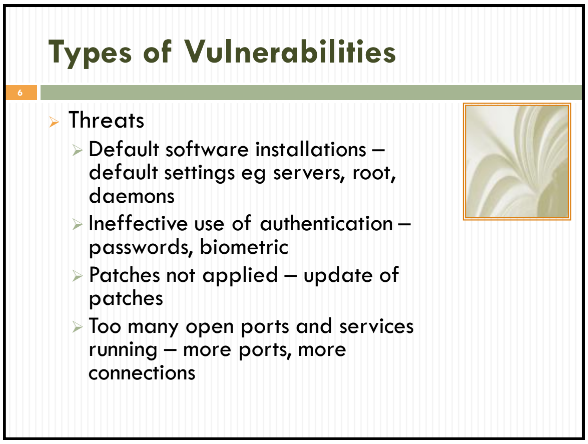
Threats

- Denial of service - flooding a network with requests that can overwhelm it and ultimately make a computer slow down or ultimately crash
- Malicious code - Trojan horses, worms, viruses
- Spoofing - making a computer look like a "trusted computer"



Types of Vulnerabilities

- Threats
  - Default software installations
  - Ineffective use of authentication
  - Patches not applied
  - Too many open ports and services running
  - Not analyzing incoming packets
  - Backups not maintained and verified
  - Lack of protection against malicious code



Types of Vulnerabilities

- Threats
  - Default software installations – default settings eg servers, root, daemons
  - Ineffective use of authentication – passwords, biometric
  - Patches not applied – update of patches
  - Too many open ports and services running – more ports, more connections

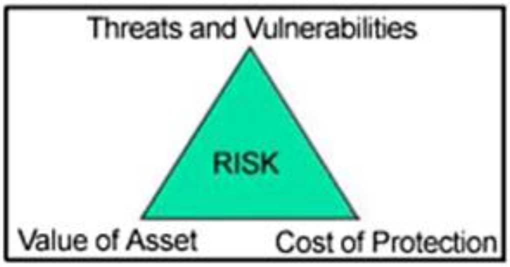
Types of Vulnerabilities

7

- Threats
  - Not analyzing incoming packets – analyzing unacceptable packets
  - Backups not maintained and verified – how many hours an asset such as server can be down
  - Lack of protection against malicious code – viruses, worms, Trojan Horses etc.

Graphs/Charts 2

8



Determining Your Assets

9

- **Assets**
  - Information and intellectual property
  - Computer hardware
  - Computer software
  - People

Assessing Your Assets

10

- **Assets**
  - **High** — Your library would suffer major disruption and legal or financial loss if the asset is attacked. Without this critical asset, your library would be sufficiently damaged as to no longer be able to fulfill its mission.
  - **Medium** — Your library would suffer minor disruption and legal or financial loss if the asset is attacked. Without this important asset, the library would still be able to fulfill its mission, but in a diminished capacity.
  - **Low** — Your library would suffer no disruption, legal or financial loss if the asset is attacked. Your library would be able to completely fulfill its mission without this trivial asset.

Creating a Security Policy Overview

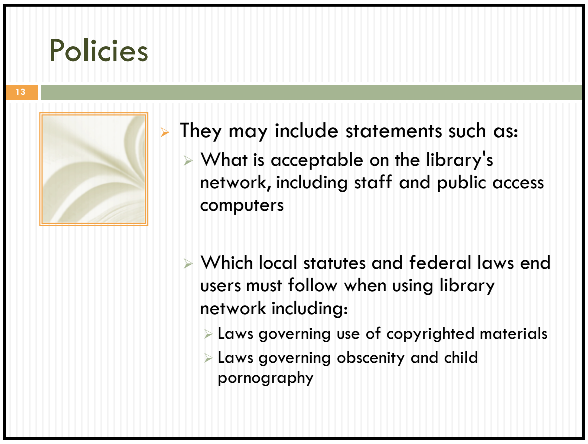
11

- **Several Preliminary Steps**
  - Create a security team
  - Develop usage policy statements
  - Review security policies from other similar organizations
  - Conduct a risk assessment

Components of a Security Policy

12

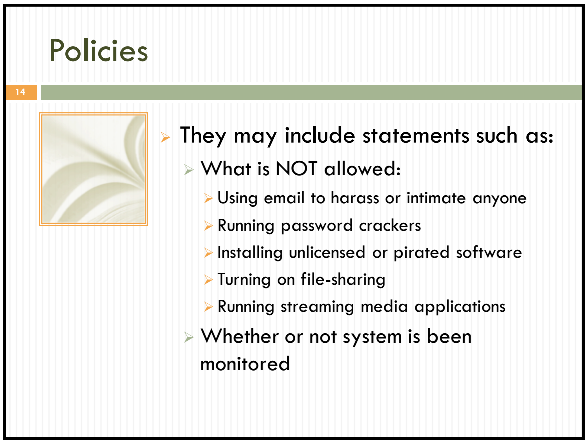
- A Security Policy has the following basic components:
  - Objective or Abstract
  - Scope
  - Responsibilities
  - Physical Security
  - Network Security
  - Software Security
  - Disaster Contingency Plan
  - Acceptable Use Policy
  - Security Awareness
  - Compliance



Policies

13

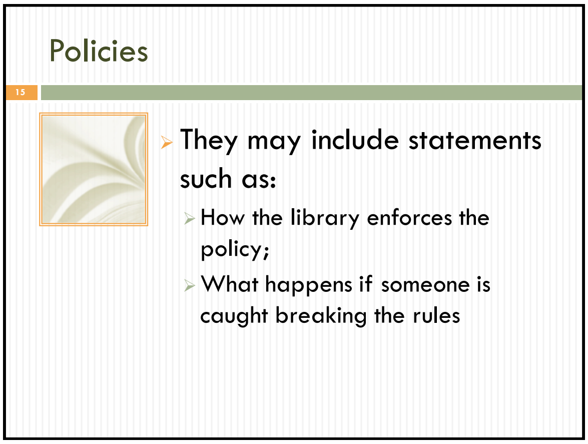
- They may include statements such as:
  - What is acceptable on the library's network, including staff and public access computers
  - Which local statutes and federal laws end users must follow when using library network including:
    - Laws governing use of copyrighted materials
    - Laws governing obscenity and child pornography



Policies

14

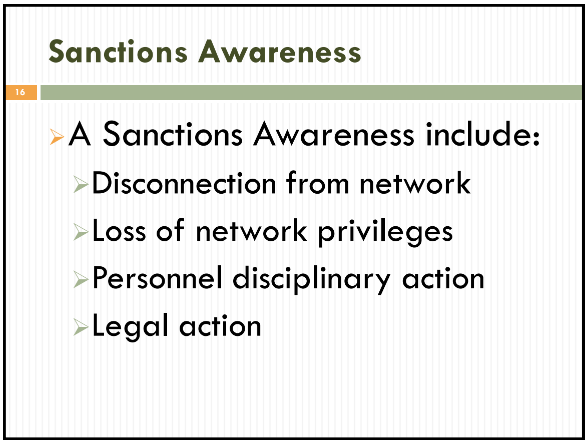
- They may include statements such as:
  - What is NOT allowed:
    - Using email to harass or intimate anyone
    - Running password crackers
    - Installing unlicensed or pirated software
    - Turning on file-sharing
    - Running streaming media applications
  - Whether or not system is been monitored



Policies

15

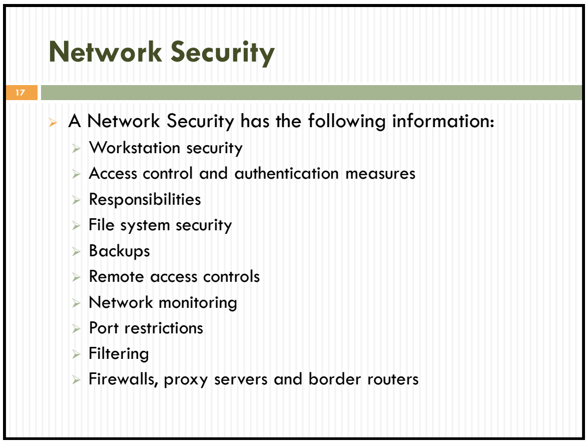
- They may include statements such as:
  - How the library enforces the policy;
  - What happens if someone is caught breaking the rules



Sanctions Awareness

16

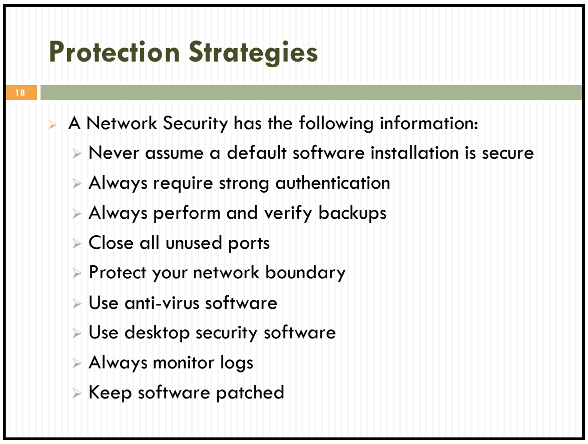
- A Sanctions Awareness include:
  - Disconnection from network
  - Loss of network privileges
  - Personnel disciplinary action
  - Legal action



Network Security

17

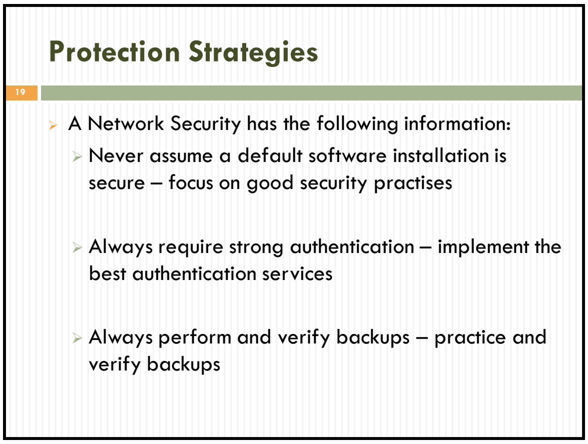
- A Network Security has the following information:
  - Workstation security
  - Access control and authentication measures
  - Responsibilities
  - File system security
  - Backups
  - Remote access controls
  - Network monitoring
  - Port restrictions
  - Filtering
  - Firewalls, proxy servers and border routers



Protection Strategies

18

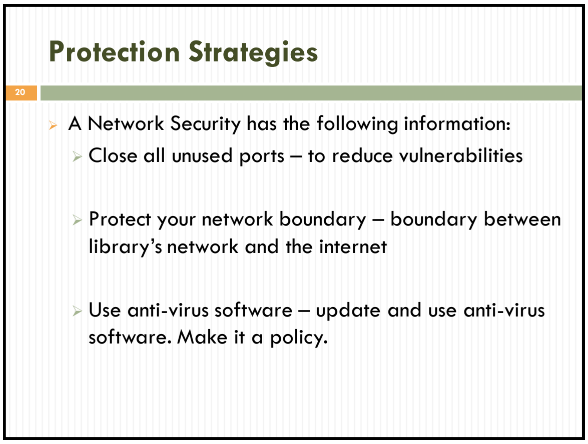
- A Network Security has the following information:
  - Never assume a default software installation is secure
  - Always require strong authentication
  - Always perform and verify backups
  - Close all unused ports
  - Protect your network boundary
  - Use anti-virus software
  - Use desktop security software
  - Always monitor logs
  - Keep software patched



Protection Strategies

19

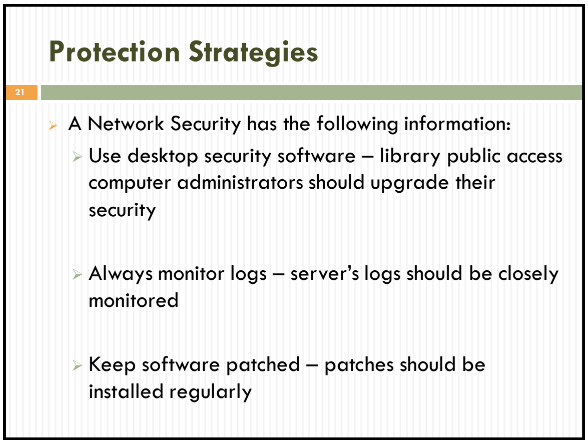
- A Network Security has the following information:
  - Never assume a default software installation is secure – focus on good security practises
  - Always require strong authentication – implement the best authentication services
  - Always perform and verify backups – practice and verify backups



Protection Strategies

20

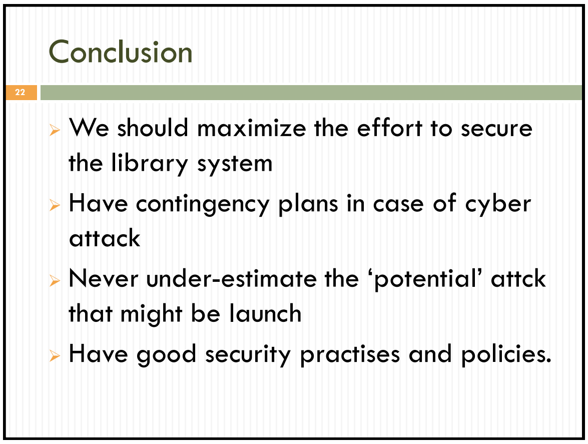
- A Network Security has the following information:
  - Close all unused ports – to reduce vulnerabilities
  - Protect your network boundary – boundary between library's network and the internet
  - Use anti-virus software – update and use anti-virus software. Make it a policy.



Protection Strategies

21

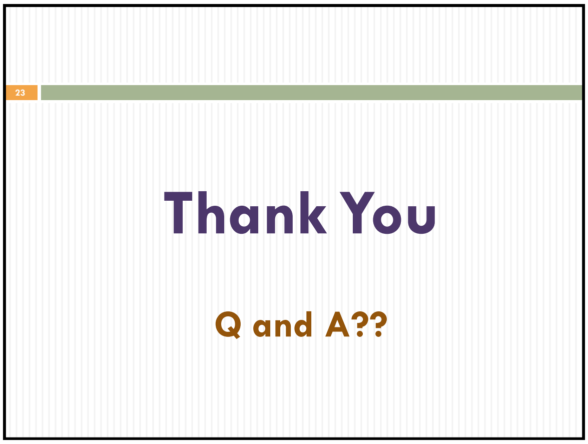
- A Network Security has the following information:
  - Use desktop security software – library public access computer administrators should upgrade their security
  - Always monitor logs – server's logs should be closely monitored
  - Keep software patched – patches should be installed regularly



Conclusion

22

- We should maximize the effort to secure the library system
- Have contingency plans in case of cyber attack
- Never under-estimate the 'potential' attck that might be launch
- Have good security practises and policies.



23

Thank You

Q and A??