A Multi-Level Protection Strategy of Information Security for Digital Library

LEI San-ya; LIU Qing-ao

The First Aeronautic Institute of the Air Force, Xinyang,464000, China

brightma@126.com

Abstract: Digital library is the trend of the future library, the opening make it easy to be invaded by net virus or illegal visitor. So the security protection of digital library is an important task. To protect the security of digital library, at first the concept of digital library is introduced, then the structure, function, service, hardware configuration and software configuration of digital library is analyzed. Base on the analysis, the security of digital library is studied from the view of operation system, network and database. Finally, a multi-level protection strategy for digital library is proposed. In this strategy, operation system configure, network protection and database protection are considered to protect digital resources which enhances the difficulty of being destroyed for the data resources. Because when one virus or a hacker invade the digital library, even the operation system or the service is damaged, other protection measure such as database protection can also act on the digital library.

Keywords: digital Library; information security; knowledge service

数字化图书馆信息安全的多层次防护策略

雷三丫，刘庆敖

空军第一航空学院，河南 信阳，464000

brightma@126.com

【摘要】数字化图书馆是未来图书馆发展的趋势，其开放性使其容易受到网络病毒及非法入侵者的危害。保护数字化图书馆的信息安全，是数字化图书馆的重要问题。为了保护数字化图书馆的安全，首先介绍了数字化图书馆的概念，然后分析了数字化图书馆的结构、功能、服务、硬件、软件等，在分析的基础上，从操作系统、网络和数据库三个方面分析了数字化图书馆的安全问题，从上三个方面，提出了数字化图书馆多层次防护的对策，该策略从多个方面，采用操作系统配置、网络防护、数据库防护等多种手段，对数字资源进行防护，增加数据被破坏的难度，降低数字资源被破坏的风险。这种多层次防护策略可以更有效地保护数字化图书馆的安全。这是因为即使当病毒或者黑客利用某个软件或者网络入侵了数字化图书馆，但由于其他层面的防护措施还起作用，从而降低了数字化图书馆的损害程度。

【关键词】数字化图书馆；信息安全；知识服务

1 引言

随着信息技术、网络技术的发展，数字化图书馆正在取代传统图书馆的一些功能。与传统的图书馆相比，除了信息量呈几何倍数增长外，经过被信息化改良过的图书馆还拥有了新的名字“数字化图书馆”。数字化图书馆是在互联网的支撑下，以内容管理为核心，以海量信息处理、知识发现与加工交流为主要技术手段的智能知识服务基础平台，是运行在互联网上的、超大规模的、便于使用的、没有时空限制的知识中心。数字图书馆是一个数字信息对象收藏，包括支持读者进行定位、检索和获取这些信息对象的服务，组织和表现这些对象的方法以及将这些对象提供给读者的相关的信息技术。美国数字图书馆提出了建设数字图书馆的八项原则，普遍得到学术界的认可。 服务是数字图书馆工作的核心。目前数字图书馆信息服务模式经过了分散分布式的“资源/产品中心”、“馆员中

978-1-935068-09-9

心”服务模式实践，正在向集中式的“读者中心”服务模式深化发展。未来的数字图书馆信息服务应该是一种以读者为中心的集成式服务，应当在服务集成、空间聚合、使用智能上下功夫。由此，个性化服务应运而生，并成为图书馆信息服务研究的新课题。

从总体上说，支撑数字图书馆的关键技术主要有信息处理、信息存储和信息传输三个方面。这种由新技术所带来的新的信息资源形态（数字化）和新的信息资源使用方式（网络传输），必然存在许多网络隐患，易受网络黑客攻击。

2 数字化图书馆

数字化图书馆以文献的数字化为标志，图书馆通过网络向每个读者提供各种数字图书、数字化期刊等资料，实现学习的数字化。数字化图书馆以网络技术、数据库技术为基础。数字化图书馆以读者的自我学习为服务对象，而个性化服务是数字化图书馆所提供服务的最重要特征。

个性化服务是数字图书馆系统中的关键部分，信息服务的智能化，由单纯的信息提供转向信息生成。数字图书馆的个性化服务主要表现为两个层次：第一层次为按读者要求进行信息订制。读者根据自己的需要订制专门信息，其功能包括数字图书馆站内搜索，Internet 搜索，时间、日期、重要事件的提示，并可帮助读者建立个性化信息空间。第二层次则是数字图书馆挖掘读者兴趣模式，主动提供服务，使数字图书馆成为一个智能型、主动性的信息提供商。数字化图书馆具有获取信息速度快、能提供新的服务形式等特点。

信息获取是图书馆的首要功能。与传统的图书馆相比，数字化图书馆个性化服务的最大优势是提高信息获取速度。数字图书馆中的信息量是庞大的，在堆积如山的数据中包含着许多待提取的有用知识。对于读者来说，他关心自己的需要是不是能够被满足更胜于关心数字图书馆中总的信息量。因此，要想为读者提供更快、更有效的服务，就必须有一套很好的搜索机制。数据挖掘技术为数字化图书馆提供了先进的信息检索工具，在数字图书馆的检索中采用数据挖掘的相关理论和方法，设计的系统将有更大的智能性。

良好便利的服务是图书馆的主要职责。数据挖掘可实现信息服务质量的提升和业务的拓展。数字化图书馆借助现代信息技术，其意义不仅在于服务媒体和时空的转变，更重要的是能够借助数据挖掘技术，完善其服务结构和提升服务水平。个性化服务的主要服务形式包括信息检索服务、定题与查新服务和信息分析服务。信息检索是数字图书馆的主要功能之一，是衡量数字化图书馆服务质量的一个重要标准。传统的检索工具缺乏结果的友好性、可理解性和交互性，往往将一大堆查询结果线性呈现，令读者不知所云。智能化的信息检索不仅支持概念检索、模糊检索、联想检索及多语言检索等，而且能迅速利用聚类算法将查询结果分析聚类，使之条理化显示，方便读者筛选，同时在此基础上确定进一步的检索定位；定题与查新服务针对科研的信息服务，其传统方式是检索文献或光盘数据库，然而在网络时代，我们更不能忽视对外部网络这一即时便利的信息发布平台的搜索，才能确保查新结果的可靠性。同时，数字图书馆可运用兴趣模式算法判断并争取潜在读者，在服务过程中，还可利用可视化技术帮助读者进行在线实时信息分析；信息分析服务直接对文本数据及其相互间的关系进行分析，从而识别出未知的、有用的知识的过程。

3 数字化图书馆数据库的安全分析

数字化图书馆的安全因素包含多方面的内容，主要是操作系统因素和网络因素。

3.1 操作系统因素

数字化图书馆中各种数字资源的存储，网络服务器的安装，都是依据特定的操作系统。因此，操作系统的安全是数字化图书馆安全的重要因素。操作系统的安全是指数字化图书馆服务器的安全，包括如 Windows NT，Windows 2000 等操作系统本身的安全性问题，而是病毒木马对操作系统的侵害等。目前应用较为广泛的操作系统有Windows、UNIX、LINIX 等等。其中 Windows 仍然是应用范围最广的系统之一。Windows 的端口是计算机与外界通讯的渠道，各类数据包在最终封包时都会加入端口信息，以便在数据包接收后拆包识别。许多蠕虫病毒正是利用了端口信息才能实现恶意骚扰的。所以，对于 Windows 系统来说，有必要把一些危险而又不常用到的端口关闭或是封锁，以保证信息安全。此外，Windows 系统中的组策略和注册表，是安全中的重要部署。很多病毒和木马都会修改注册表，使系统无法正常工作。

3.2 网络因素

网络因素是数字化图书馆数据安全的重要因素。由于数字化图书馆依赖于网络载体存在，所以网络所面临的安全性问题，数字化图书馆同样具有。数字图

书馆的性质决定了其对网络的依赖性。网络的安全稳定运行是数字图书馆正常运行的前提，电子期刊、电子图书、多媒体资源的传输都是由网络进行传输的，网络传输的稳定性、安全性，将影响到数字资源的使用。

一般而言，网络安全包括硬件安全和软件安全两个方面。网络的硬件安全是数字化图书馆的存储仓库，是数据传输的通道，硬件的稳定与否，关系着数字化图书馆的服务质量。比如服务器的性能，当大量用户同时访问数据库时，会产生大量的查询、下载请求，等待时间取决于服务器的速度。因此，服务器的性能需要根据访问客户的平均数量或最大数量来决定，既没有必要追求高性能，也不能仅从价格上考虑。可以通过调查数字化图书馆的访问量，来决定服务器的运行速度。软件安全主要包括数字化图书馆服务器所安装的杀毒软件、网络防火墙，甚至包括数字化图书馆的服务策略。由于数字化图书馆采用网络服务的方式，所以操作系统的安全，也与数字化图书馆的安全密切相关。因此，操作系统的补丁要及时更新。杀毒软件的病毒库和网络防火墙都需要及时进行更新。另外，数字化图书馆的服务策略，也可能会导致服务瘫痪。例如，部分恶意程序可以长时间大量请求，占用系统服务资源，使其它用户不能正常访问，也会影响数字化图书馆的服务。

3.3 数据库因素

数字化图书馆数据库是数字化图书馆的主要组成部分，保护数据库的安全是建设数字化图书馆的重要部分。当然，安全的概念是相对的，任何一个系统都具有潜在的危险，没有绝对的安全。在一个特定的时期内，在一定的安全策略下，系统可能是安全的。但是，随着攻击技术的进步、新漏洞的暴露，系统可能会变得不安全了。由于数字化图书馆采用了计算机网络技术，所以其安全性包括了物理层、网络层、系统层、应用层以及管理层等多个方面。从技术上来说，系统的安全是由安全的软件系统、防火墙、网络监控、信息审计、通信加密、灾难恢复、安全扫描等多个安全组件来保证的，单独的安全组件只能提供部分的安全功能，无论缺少哪一个安全组件都不能构成完整的安全系统，而数据库的安全是数字化图书馆安全的重中之重。

由于数字化图书馆的数据库包含大量的电子期刊、电子图书、影像视频资料，所以数字化图书馆的安全性也就是数字资源的安全性，这些数字资源又是以数据库的形式存在，所以数字化图书馆的安全性问题包含网络数据库的安全。另外，由于数字化资源的存储介质的不稳定性问题，也是影响数字化图书馆安全的重要因素。比如磁盘的长时间使用，会是部分磁道发生损害，丢失数据。

数据库系统安全包含运行安全和信息安全。数据库系统运行安全包括：法律、政策的保护，如用户是否有合法权利，政策是否允许等；物理控制安全，如机房加锁、安全审批等；计算机硬件运行安全；操作系统安全，如数据文件是否保护等；灾害、故障恢复；死锁的避免和解除；电磁信息泄漏防止。数据库系统信息安全包括用户口令字鉴别、用户存取权限控制、数据存取权限、方式控制、审计跟踪、数据加密等。

4 安全对策

4.1 操作系统安全

从操作系统的安全性考虑，数字化图书馆的服务器应当关闭一些不常用的端口，避免受到黑客和木马的攻击。另外，数字化图书馆服务器的安全性需要及时更新操作系统的补丁，及时更新杀毒软件，正确配置操作系统。

4.2 网络安全

网络攻击技术包括目标网络信息收集技术，目标网络权限提升技术，目标网络渗透技术，目标网络摧毁技术四大类。对数字化图书馆而言，不管其是否已经受到这些攻击，不管这些攻击是否产生了比较严重的后果，都必须假设它们对信息系统的威胁总是存在的。因此在任何时候，对数字化图书馆信息系统的连续不断的保护是非常必要的。而对攻防技术发展和网络安全实践的研究分析表明，单一的安全保护往往效果不理想，而最佳途径就是采用多层安全防护措施对信息系统进行全方位的保护。

所谓“多层次防护”，就是应用和实施一个基于多层次安全系统的全面信息安全策略，在各个层次上部署相关的网络安全产品，增加攻击者侵入所花费的时间、成本和所需要的资源，从而卓有成效地降低被攻击的危险，达到安全防护的目标[1]。多层防护的策略实际上就是结合不同的安全保护因素，例如防病毒软件、防火墙和安全漏洞检测工具，来创建一个比单一防护有效得的多的综合的保护屏障。分层的安全防护成倍地增加了黑客攻击的成本和难度，从而大大减少了他们对数字化图书馆的攻击。多层防护在具体应用中能够层层高度戒备，已经成为当今网络安全的主流策略。

978-1-935068-09-9 © 2010 SciRes.

分层的安全防护技术具体来说包括攻击检测，攻击防范，攻击后的恢复这三个大方向。入侵检测系统负责进行攻击检测，防火墙和强制访问控制系统负责攻击防范，攻击后的恢复则由自动恢复系统来解决。这三大方向就说明了在网络安全防护上的多层安全防护措施。因此，数字化图书馆应该使用可以进行自动回复的操作系统，并且具有入侵检测和防火墙等功能，实现多层次的防护，最大限度地保证数字资源的安全。

4.3 数据库安全对策

一个数据库能否防止无关人员得到他不应该知道的数据，是数据库是否实用的一个重要指标。如果一个数据库对所有的人都公开数据，那么这个数据库就不是一个可靠的数据库。数字化图书馆的数据应该设置访问权限，只允许部分管理人员可以访问全部数据。因此，数字化图书馆的数据库应采取以下措施：

（1） 使用授权规则

这是数据库系统经常使用的一个办法，数据库给用户 ID 号和口令、权限。当用户用此 ID 号和口令登录后，就会获得相应的权限。不同的用户或操作会有不同的权限。比如，对于一个表，某人有修改权，而其他人只有查询权。

（2） 将数据加密，以密码的形式存于数据库内

此外，数字化图书馆要采用并发控制技术，防止非法用户占用合法资源。如果数据库应用要实现多用户共享数据，就可能在同一时刻多个用户要存取数据，这种事件叫做并发事件。当一个用户取出数据进行修改，修改存入数据库之前如有其他用户再取此数据，那么读出的数据就是不正确的。这时就需要对这种并发操作施行控制，排除和避免这种错误的发生，保证数据的正确性。

最后，当数据库系统运行时出现物理或逻辑上的错误时，如何尽快将它恢复正常，这就是数据库系统的故障恢复功能。一般而言，数据库系统提供的上述基本安全技术能够满足一般的数据库应用，但对于军队数字化图书馆，仅靠上述这些措施是难以完全保证数据库的安全性的，某些用户尤其是一些内部用户仍可能非法获取用户名、口令字，或利用其他方法越权使用数据库，甚至可以直接打开数据库文件来窃取或篡改信息。备份对数据库的安全来说是至关重要的。数据库的备份应该什么时候做，用什么方式做，主要取决于数据库的不同规模和不同的用途。恢复或重载也是保护数据库安全的重要措施之一，周期性地（如 3 天一次）对整个数据库进行转储，把它复制到备份介质中（如磁带中），作为后备副本，以备恢复之用。或者对数据库的每次修改，都记下修改前后的值，写入“运行日志”数集中。它与后备副本结合，可有效地恢复数据库。

5. 展望

随着数字化图书馆技术的成熟，其安全性也受到广泛的重视。网络攻击工具的复杂化、成熟化、自动化和智能化给数字化图书馆数据库的安全带来更大的挑战。数据库的安全仅仅是数字化图书馆安全的一部分，系统的安全需要多种安全防范政策、防范措施的保护，才能保证数字化图书馆整体的安全。本文提出的多层次防护策略，从操作系统、网络安全、数据库防护多个方面对数字化图书馆进行信息安全防护。该防护策略增加数据被破坏的难度，降低数字资源被破坏的风险。

References (参考文献)

[1] Sudha Ram , Jinsoo Park , Dongwon Lee, Digital Libraries for the Next Millennium: Challenges and Research Directions[J], Information Systems Frontiers, v.1 n.1, p.75-94, July 1999.

[2] Li Yu, Liu Jingsen, Mechanism and Improvement of Direct Anonymous Attestation Scheme[J], *Journal of Henan University*, 2007, 37(2), P195-197 (Ch).

[3] Leonardo Candela , Donatella Castelli , Pasquale Pagano, A reference architecture for digital library systems: principles and applications, Proceedings of the 1st international conference on Digital libraries: research and development, February 13-14, 2007, Pisa, Italy.

[4] Dale Tesch/Greg Abelar .*Security Threat Mitigation and Response: Understanding CS-MARS*[M]. Cisco Press, Sep. 26, 2006.

[5] Konstantinos Xinidis, Ioannis Charitakis , Spiros Antonatos , Kostas G. Anagnostakis , Evangelos P. Markatos, An Active Splitter Architecture for Intrusion Detection and Prevention[J], IEEE Transactions on Dependable and Secure Computing, v.3 n.1, p.31, January 2006.

[6] Tzu-Fang Sheu , Nen-Fu Huang , Hsiao-Ping Lee, Hierarchical multi-pattern matching algorithm for network content inspection[J], Information Sciences: an International Journal, v.178 n.14, p.2880-2898, July, 2008.