高校图书馆多校区网络安全防御体系的构建

王春梅 孔繁之

（济宁医学院图书馆 济宁 272013） （济宁医学院信息工程学院 济宁 272013）

〔摘要〕 从多校区图书馆网络现状入手，分析多校区图书馆网络存在的安全隐患和影响网络安全的主要因素，从网络安全技术应用、网络安全管理制度建立两方面，论述多校区图书馆网络安全防御体系的构建。

〔关键词〕 多校区图书馆；网络安全；安全防御

Constructing Network Safety Defensive System in Multi – campuses of College and University Libraries *WANG Chun – mei*, *Library of Jining Medical University*, *Jining 272013*, *China*; *KONG Fan – zhi*, *Information Engineering School of Jining Medical University*, *Jining 272013*, *China*

〔**Abstract**〕 The paper starts with current network status in libraries of the multi – campuses in colleges and universities, then analyzes the existing security risks and the main factors that might affect network safety, discusses the construction of network safety defensive system from two aspects: applying network safety technology and constructing the network safety management system.

〔**Keywords**〕 Multi – campus libraries; Network security; Security defense

随着我国高等教育体制改革的不断深入，兴起了一股高校合并浪潮，一批高校为了扩大招生规模，兴建新校区，这就形成了一个高校拥有分布在不同地理位置上多个校区图书馆的格局。因图书馆信息资源共享及业务管理同步的需要，多个校区图书馆之间必须通过校园网、Internet 网组成一个有机的整体，从而多校区图书馆网络安全问题便成为高校图书馆技术人员急需解决的问题。本文从多校区图书馆网络现状入手，分析网络系统存在的安全隐患，结合实践经验，提出了多校区图书馆网络安全防御体系的构建方案。

1 多校区图书馆网络现状

1.1 多校区图书馆的管理模式

大多数多校区图书馆之间采用“总分”管理的模式，即以校本部图书馆作为总馆，其他校区的图书馆作为分馆。资源建设大多由总馆统一管理，如图书采购、编目、电子资源的采购、安装、维护等；分馆主要负责读者的信息服务，如图书借还、参考咨询等。各图书馆之间不仅要达到电子资源的共享，还要实现图书的通借通还，本校读者能够在任一校区查到馆藏书目信息和本人借还信息，这就要求总馆采编信息和各馆的流通信息通过图书馆内部业务管理系统实现异地实时数据共享，并保持各馆数据更新的同步[1]。

1.2 多校区图书馆网络的特点

多校区图书馆要实现各馆之间馆藏书目数据、流通数据和读者信息的同步，必须打破独立馆舍时图书管理系统只在馆内局域网内传递信息的局限，

〔收稿日期〕 2010 – 04 – 20

〔作者简介〕 王春梅，本科，主任，副研究馆员，发表论文 10 余篇。

需通过校园网与 Internet 连接，在广域网、城域网之间进行信息传递。因此多校区图书馆的网络系统是整个 Internet 的缩影，具有分布的广域性、体系结构的开放性、资源的共享性和信道的公用性等特点，使得多校区图书馆不得不面临网络系统安全这一严峻挑战[2]。

2 影响多校区图书馆网络安全的主要因素

2.1 网络安全不受重视

许多高校图书馆领导把资源建设作为重点，投入大量资金购买各种电子资源及存储设备，而对网络安全防护的投入有限，网络设备的冗余性较差，安全措施不到位，故障率高[3]。有的甚至没有购置和安装网络杀毒软件和防火墙。在安全管理方面还只是停留在故障管理、配置管理等传统网络管理上，对网络安全管理人员没有培训计划。

2.2 安全防范意识淡薄

在高校图书馆中，许多工作人员缺乏计算机的安全操作常识，网络管理员对各个部门和工作人员使用机器的权限设置不细致，有的权限过大；对服务器和核心设备设置的密码太弱，没有严格的账号认证制度；不及时检测操作系统及应用软件漏洞；缺少对图书馆工作人员的网络安全教育和培训，没有形成有效的网络安全防范制度，且存在制度执行不严的情况。

2.3 病毒感染

随着计算机网络的迅速发展，许多恶性病毒都是通过网络进行传播，对带宽分布结构比较脆弱的多校区图书馆网络的正常运行，造成严重的危害[4]。大学图书馆都有一批直接接入校园网的电子阅览室，在很大程度上满足了读者对文献信息检索的需求，同时也成为网络病毒滋生的温床[5]。为教职工传输文件方便，图书馆及校园网都设置 FTP 服务器，这为病毒的传播提供了方便，也给图书馆计算机网络的安全工作带来更大的难度。

2.4 网络攻击

由于多校区图书馆网络具有分布的广域性、体系结构的开放性，造成黑客的攻击不仅仅来自校园网内部，大多数来自外部。网络安全的最大威胁来自于黑客对图书馆网络系统的攻击。黑客往往会有选择地破坏图书馆之间传播网络信息的有效性和完整性，或伪装为合法用户进入图书馆网络系统，窃取重要信息，修改书目数据、流通数据和读者信息，删除电子资源，破坏图书馆网站[6]。黑客入侵的主要手段有两种，一种是窃取用户的口令，在合法身份的掩护下进行非法操作；另一种是利用网络操作系统的某些合法但不为系统管理员和合法用户所熟知的操作指令。

3 构建多校区图书馆网络安全防御体系

3.1 应用网络安全技术

3.1.1 *VPN 技术* 核心是采用隧道技术，主要负责将内部网络的数据经过加密、协议封装和压缩处理后再嵌套入另一种协议的数据包，送入虚拟公网隧道中，像普通数据包一样进行传输[7]。多校区图书馆间图书实行通借通还，并要求书目信息、流通信息准确、及时、安全。多校区图书馆可租用本地公网的宽带线路，利用 VPN 技术，将总馆与各分馆之间构建若干条虚拟专用网络，这样总馆和各分馆之间就形成了一个仿真的内部网络，各馆之间的数据可以像在同一馆内自由传递，从而实现图书馆内部管理网络的互联。

3.1.2 *虚拟局域网（VLAN）技术* 多校区图书馆网络涉及内外网不同层面的网络服务，仅采用主机安全保护方案是远远不够的，在攻击者的非法访问到达主机之前就应受到网络的拒绝。因此，还需要图书馆网络进行安全访问控制。采用 3 层交换机的路由功能，对于多校区图书馆网络内的节点，根据其功能及工作性质的不同，将其划分到不同的虚拟子网中，并对每个 VLAN 赋予不同的对外访问权限。如将各馆业务管理系统使用的计算机划在 VLAN1，电子阅览室读者用计算机划分在 VLAN2，

Web 服务器、FTP 服务器、E - mail 服务器、电子资源存储服务器划分在 VLAN3，提供书目查询、读者信息查询、信息检索和电子资源利用的计算机划分在 VLAN4，需要连接校园网的办公用计算机划分在 VLAN5[8]。

3.1.3 安装防火墙 保护整个内部网络不受外界入侵影响，最佳的选择还是使用防火墙。利用防火墙的包过滤、应用代理、网络地址转换、身份认证、权限控制、安全审计、攻击检测、流量控制等功能，为图书馆网络提供一整套从网络层到应用层的安全解决方案。通过对防火墙的合理配置，使它成为被保护网络与外部网络之间的一道屏障，阻止不可预测的潜在破坏性入侵，从而实现对图书馆网络的安全保护。

3.1.4 采用入侵检测系统 对计算机网络系统中收集的若干关键信息进行分析，从中发现是否有违反安全策略的行为和被攻击的迹象。在有内部非授权行为或外部攻击行为时，及时发现、记录并发送报告，以便网络管理员采取进一步措施来保护网络。其主要完成以下功能：监视、分析用户及系统活动；系统构造和弱点审计；识别已知攻击的活动模式并进行报警；异常行为模式统计分析；评估重要系统和文件的完整性；操作系统的审计跟踪管理；并识别用户反安全策略的行为。一个入侵检测系统应能使安全管理员时刻了解网络系统的任何变更，还能给网络安全策略的制订提供指南[9]。

3.2 建立健全图书馆网络安全管理制度

3.2.1 建立用户网络安全教育制度 高校图书馆主要用户是学生，图书馆内部的网络攻击也主要来自学生，因此加强对学生的网络安全教育是解决图书馆网络安全问题最简单有效的途径。应将网络安全教育作为新生入馆教育的一个重要内容，也可通过举办网络安全教育培训讲座形式，以增强学生的网络道德意识、法律意识及责任感。

3.2.2 制定操作规程 加强对工作人员网络安全教育和培训，增强网络安全意识和防范能力。制定工作站操作员操作规程，并严格执行。严格工作人员口令管理，禁止外人使用工作人员的电脑，工作人员不准私自安装与工作无关的各种程序，强制工作用机定期查杀病毒。对于图书业务管理系统的专用计算机，不准使用 U 盘，出现任何故障及时向网络管理员汇报，不得自行处理。

3.2.3 建立安全管理制度 建立机房管理制度，严格限制无关人员的出入。严格执行口令保密制度，严禁将口令外泄。建立用户权利分级管理制度，制定完备的系统维护制度，合理设置软、硬件防火墙及其他网络设备。建立完整的病毒防御体系，在电子阅览室和公共查询机上安装硬盘保护卡，防止病毒在读者用机上传播。建立灾难备份恢复机制，制定切实可行的网络安全应急方案，以应对各种网络安全威胁的来临。

图书馆网络安全是一项系统工程。图书馆应加大网络安全设施的投入，并对这些网络设施和系统进行合理配置和利用，提高网络安全防御的能力，同时还要有一套严格科学的安全管理制度和切实可行的应急措施。只有将技术和管理制度有机结合，才能构成一套行之有效的多校区图书馆网络安全防御体系，图书馆的网络安全才能落到实处。

参考文献

1 刘明昕. 基于 VPN 技术的多校区高校图书馆网络问题研究〔J〕. 现代情报，2009，(12)：78 - 81.

2 林昌意. 多校区图书馆网络安全防范体系的实施〔J〕. 太原师范学院学报，2008，(4)：59 - 63.

3 刘炳芳. 构建高校图书馆网络安全防护体系〔J〕. 网络财富，2008，(6)：109 - 111.

4 岳江红. 一种多校区校园网的整网安全解决方案〔J〕. 北京联合大学学报，2007，(3)：37 - 40.

5 李腾. 高校数字图书馆的数据安全与保障措施〔J〕. 科技情报开发与经济，2009，(12)：9 - 11.

6 尹志清. 高校图书馆网络安全体系的构建〔J〕. 武汉船舶职业技术学院学报，2007，(1)：41 - 43.

7 王朗. 利用 VPN 技术实现合并图书馆分馆互联〔J〕. 现代图书情报技术，2004，(5)：35 - 37.

8 路莹. 构建基于三层交换技术的图书馆 VLAN 网络〔J〕. 中华医学图书情报杂志，2008，(1)：60 - 63.

9 王福生. 图书馆网络中的入侵检测系统〔J〕. 现代情报，2007，(7)：35 - 36.