第56卷 第5期
2003年9月

武汉大学学报(社会科学版)
Wuhan University Journal (Social Sciences)

Vol.56.No.5
Sept. 2003.648~652

■图书情报学

# 解决数字图书馆信息资源安全问题的TOR模式

胡昌平，周朴雄
(武汉大学 信息管理学院，湖北 武汉 430072)

[作者简介] 胡昌平(1945-)，男，湖北枝江人，武汉大学信息管理学院情报学系教授，博士生导师，主要从事信息管理学研究；周朴雄(1972-)，男，湖北松枝人，武汉大学信息管理学院情报学系博士生，主要从事信息管理安全与应用研究。

[摘 要] 数字图书馆普遍面临着信息资源安全问题，针对这一现实问题拟从安全技术、安全组织管理和安全法律法规三方面出发构建解决其信息资源安全的完整体系。

[关 键 词] 信息资源安全；TOR对策；数字图书馆
[中图分类号] G250.76 [文献标识码] A [文章编号] 1671-8828(2003)05-0648-05

## 一、数字图书馆所面临的安全问题

数字图书馆是一个宽带多媒体网络和大量信息管理系统，它将信息数字化后存贮起来，以网络为基础进行信息传递，为本地区或远程读者提供服务。由于计算机网络分布的广域性、开放性和信息资源的共享性，为信息的窃取、盗用，非法的增删改及种种扰乱破坏，提供了极为方便且难以控制的可乘之机，数字图书馆信息服务的权益保护及监督问题得不到有效的保障；同时，由于计算机网络的脆弱性，数字图书馆的网络系统本身经常处于黑客的攻击之中。因此，安全问题是数字图书馆的核心问题之一，它关系到数字图书馆的使用、推广和发展。就目前的现状来看，数字图书馆所面临的安全问题主要有以下几个方面：

1.口令攻击。当前，无论是数字图书馆的用户，还是系统管理员，都是用口令来维护他们的安全，通过口令来验证用户的身份。发生在数字图书馆上的入侵，许多都是因为系统没有口令，或者用户使用了一个容易猜测的口令，或者口令被破译[1](第225-263页)。

2.拒绝服务的攻击。拒绝服务攻击的英文是Denial of Service，简称DoS。这种攻击行动使数字图书馆服务器充斥大量要求回复的信息，消耗网络带宽或系统资源，导致其网络或系统不胜负荷以至于瘫痪而停止提供正常的网络服务[2](第165-263页)。

3.网络监听。网络监听是指黑客们利用监听工具监听数字图书馆网络的状态、数据流动情况以及网络上传输的信息。网络监听可以在网上的任何一个位置，如果黑客通过监听截获用户或管理员的口令，则可以非常容易地登录到数字图书馆网络系统[3](第7\|11页)。

4.欺骗。欺骗是一种积极的攻击方式，在这种情况下，网络上的某台机器伪装成另一台不同的机器。作为一种主动的攻击，它能破坏两台机器间通讯链路上的正常数据流并可能向该链路上插入数据。其目的在于哄骗网络上的其他机器将冒名顶替者作为原始机器加以接受，诱使其他机器向它发送数据或允许它修改数据[1](第225-263页)。

收稿日期：2003-04-17
基金项目：国家教育部重大项目(2000ZDXM870001)

5.其他攻击方法。其他攻击方法主要是利用一些程序进行攻击，比如后门，程序的逻辑炸弹和时间炸弹、病毒、蠕虫、特洛伊木马程序等。其中，病毒对数字图书馆的威胁最大，病毒主要通过传染和复制来破坏系统。首先通过修改或者覆盖引导扇区或主引导记录的程序以及在目标文件上附加恶意的代码程序，这样，病毒的原始代码被附加到受侵蚀的文件上。这个被过程称为感染。从那个时候开始，这被个感染的文件又能感染其他文件。这个过程称为复制。通过复制，病毒能够通过网络进行传播，达到摧毁系统的目的[4]（第 8—17 页）。

总之，目前数字图书馆信息资源所面临的安全问题是复杂的、全方位的。有的是由于数字图书馆信息网络所采用的安全技术不能有效地防止黑客的攻击造成的；有的是由于所采用的安全管理措施不得力所造成的；也有的是由于没有一套合理的安全管理法规或政策所造成的。这些就决定了在解决数字图书馆信息资源的安全问题时必须采用多种方法，进行综合地、全方位地考虑。

## 二、现有解决方法的局限性

由于数字图书馆所面对的存储对象和技术领域远远超出了传统图书馆所涉及的范围，其安全问题领域很宽广，需要大量的技术突破和管理方法作为支撑。目前，国外较为成熟的安全技术有密码理论与技术，安全协议理论与技术，安全体系结构理论与技术，信息对抗理论与技术。我国在密码学领域的研究以及反病毒、防火墙和入侵检测等安全产品的研究与开发方面已经较为成熟。以美国为首的国际安全组织已经制定出了比较全面的安全标准和法规。我国从 21 世纪 80 年代起，参照国际标准也制定了一系列的安全标准和法规。这些技术理论、标准和法规为解决数字图书馆信息资源的安全问题提供了支撑和依据。

从国际上来看，在将传统安全技术（如安全身份论证技术、主机入侵检测技术等）应用于数字图书馆方面已经取得进展，但是，许多数字图书馆在某种程度上来说，还只是局限于从技术层面来解决问题。如美国国家科学基金会正在开发一座大型网上数字图书馆，这座被称为 NSDL 的图书馆就涵盖了目前比较先进的网络安全技术，并对这些技术进行过二次开发，但与之对应的安全管理及法规的发展却相对滞后一些。我国的数字图书馆也开始逐渐地采用一些国内外的先进安全技术和安全对策来解决其安全问题，但大多只是针对于有限的几种安全威胁，对于来自于系统硬件以及网络协议的更多的安全问题也无能为力。所使用的安全产品的功能本身就存在诸多不够完善的地方，也很少进行针对数字图书馆的特定情况的有效的二次开发。再就是信息资源的安全管理问题没有得到足够的重视，数字图书馆的管理人员和用户的安全意识和自我保护能力还很薄弱。

总之，从国内外的研究状况来看，目前对于数字图书馆的安全问题的研究仍然处于分散状态，未能对其进行系统研究。各数字图书馆在解决安全问题时，大多只局限于从技术或管理的某一方面去解决，没有一套完整的解决方案。因此，很有必要从数字图书馆的安全技术、安全管理、安全法规与政策等各个方面进行研究，解决其中的关键问题，从底层技术到高层应用搭建起数字图书馆的安全体系和模式，来综合地、全方位地解决数字图书馆的安全问题。

## 三、TOR 模式

数字图书馆信息资源安全问题的解决需要从现有的网络安全技术出发，针对数字图书馆的实际情况对这些技术进行二次开发，从技术层面构建其系统安全平台，并进一步提出基于该平台的数字图书馆安全管理机制和模型，对用户和图书馆系统管理人员的权限进行规范。最后，提出数字图书馆安全管理的有关安全法规和政策。为此，本文提出解决数字图书馆信息资源安全问题的 TOR 模式。

TOR 模式试图从全方位解决数字图书馆信息资源安全涉及的问题。它包括三个环节：T

(Technology)环节是数字图书馆信息资源安全所包含的各种技术;O(Organization)环节是数字图书馆信息资源安全实施中的组织与管理问题;R(Regulation)环节是与其相关的各种法律、法规。其中技术是发展数字图书馆信息资源安全的基础;组织是保障;法律是准绳[5](第 45-78 页)。本文将对这三个基本环节进行分析,构成完整的解决方案,从而形成解决数字图书馆信息资源安全问题的 TOR 模式。

(一)安全技术(T)环节

数字图书馆信息资源安全是一项动态的、整体的系统工程,从技术上来说,数字图书馆网络安全由安全的操作系统、防病毒、防火墙、入侵检测、网络监控、通信加密、安全扫描等多个安全组件组成,一个单独的组件是无法确保数字图书馆网络的安全性的。为此从技术上提出数字图书馆网络的安全系统平台结构如图 1[2](第 165-243 页)。

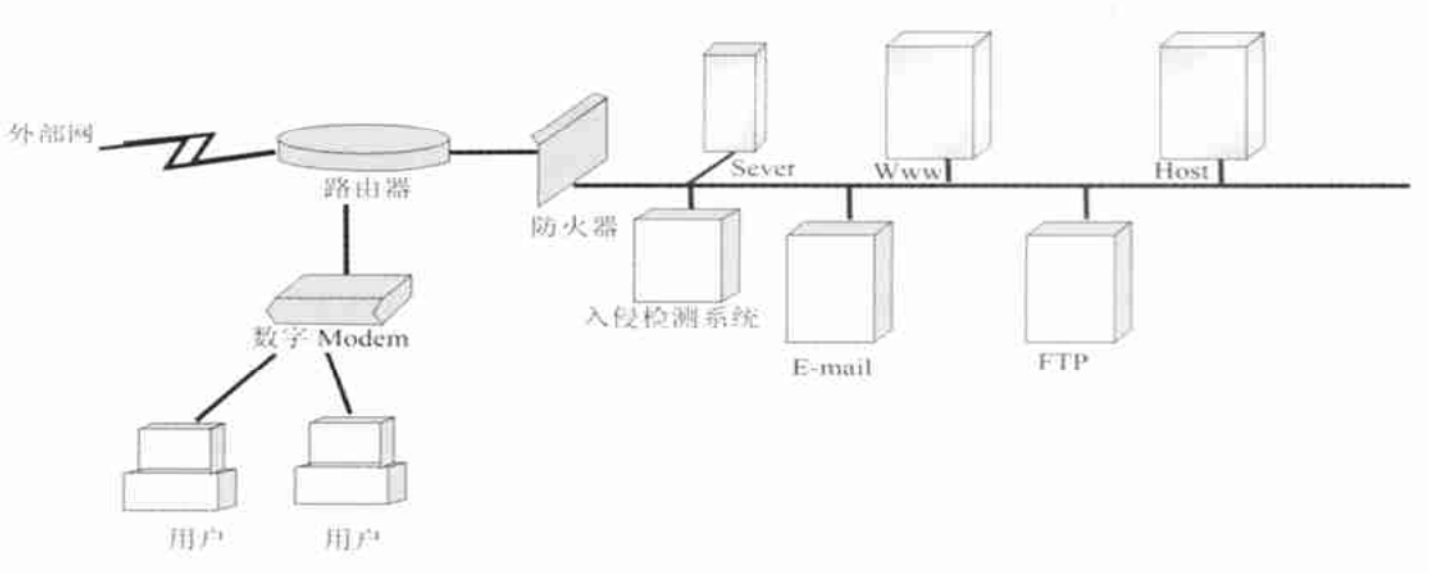


图 1 数字图书馆网络安全系统平台结构

从图 1 中可以看出,该平台包括防火墙子系统、防病毒子系统、入侵检测子系统等。应用防火墙技术可以控制访问权限,实现对数字图书馆网络安全的集中管理;其主要作用是在网络入口处检查网络通讯,使数字图书馆内部网络与外部网络实现有效的隔离,所有来自外部网络的访问请求都要通过防火墙的检查,这样内部网络的安全性便得以提高。应用入侵检测系统可以保护网络与主机资源,防止来源于内外网的攻击,提供实时的入侵检测及采取相应的防护手段,如记录证据用于跟踪和恢复、断开网络连接等。另外,在数字图书馆的计算机网络系统还应安装防病毒系统,建立全面的网络防病毒体系。

(二)安全组织(O)与管理环节

安全组织(O)与管理是数字图书馆信息系统安全的重要组成部分。数字图书馆信息系统安全,不仅要依赖所采用的安全技术防范措施,而且要看它所采取的安全管理措施。数字图书馆信息系统的安全管理,包括建立相应的安全管理机构、不断完善和加强计算机系统的管理功能、实施计算机系统本身的安全管理等方面。其目的是利用各种措施来支持数字图书馆信息系统的安全策略和安全机制的实施及完善,作出与安全有关的信息报告及相关事件的记录,以便审计追踪和依法处理。

1.建立数字图书馆信息资源的安全管理机构(包括安全审查机构、安全决策机构、安全管理和领导机构等),对系统安全任务的落实是十分必要的。安全审查机构主要负责收集对系统资源的各种非法访问事件,监视系统的运行情况,并对非法事件进行记录,分析和处理。必要时,将审计的事件及时向安全领导机构的领导报告等。安全决策机构负责制定数字图书馆系统内的安全决策和安全机制,以及有关的安全规章制度。

2.完善和加强数字图书馆计算机系统的安全管理功能,首先,应加强对数字图书馆用户账号和口令的管理,设置对文件、目录、打印机和其他系统资源的访问权限,加强口令滚轮,设置其有效期,根据需要经常更改口令等。其次,应加强对计算机的监控能力,使其具有智能化,确保审计系统能记录所有访问

尝试和使用的活动情况。系统管理员应不断收集和积累有关的安全事件记录并加以分析，选择其中的某些用户进行审计跟踪，以便对发现的或可能产生的破坏性行为提供有力证据。最后，也可以通过网络文件进行严格的访问控制，达到控制用户行为的目的[3]（第 7-11 页）。

3．数字图书馆计算机系统本身的安全管理，数字图书馆计算机系统本身的安全管理应贯穿于系统设计和系统运行的各个阶段。在设计阶段，在系统软、硬件设计的同时，应制定系统的安全策略和安全机制；在系统运行中，要贯彻、执行安全机制所要求的各项措施和安全管理原则，并经风险分析和安全审计来检查、评估，并不断改进和完善各种安全措施。数字图书馆的安全管理主要有三条基本原则：一是从不单独活动原则，在人员条件允许的情况下，由数字图书馆馆长指定两个或更多的，可靠且能胜任工作的专业人员，共同参与每项与安全有关的活动，并通过签字、记录、注册等方式来证明。二是限制使用期限原则，任何人都不能在一个与安全有关的岗位上工作太长的时间。三是责任分散原则，不集中于一人实施全部与安全有关的功能[6]（第 148-158 页）。

（三）法律与规章（**R**）环节

法律与规章（R）环节与 T 环节、O 环节相辅相成，安全技术与安全管理是基础，而法律与规章（R）是数字图书馆所采用的安全技术和安全管理的法律化，是技术与管理的保障，它反映了高科技立法的特征，有利于数字图书馆的管理人员和用户认真地、自觉地执行安全措施，并提高在这方面的管理水平，增强安全防范意识。它包括与数字图书馆信息资源安全相关的各种安全法律、安全管理制度和安全技术标准。目前，随着数字图书馆的兴起，针对数字图书馆信息资源的计算机犯罪、黑客攻击、计算机病毒等案件不断出现。这在一定程度上是由于相关法律、法规不健全，制裁不力造成的。所以，应不断加强有关数字图书馆信息资源安全的立法和执法力度，来对付这些犯罪，保证数字图书馆信息资源的安全。

首先，应加强有关数字图书馆信息资源安全的标准、规章及法律的建设。目前，已经有了关于信息资源安全的国际标准、规章及法律。国内主要是采用等同国际标准。由公安部主持制定、国家质量技术监督局发布的中华人民共和国国家标准 GB17895-1999《计算机信息系统安全保护等级划分准则》已正式颁布并实施。该准则将信息系统安全分为 5 个等级：自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级。主要的安全考核指标有身份认证、自主访问控制、数据完整性、审计等，这些指标涵盖了不同级别的安全要求。在信息犯罪方面，对计算机犯罪、黑客攻击、计算机病毒已经制定了相应的法律。我们要以这些安全标准、规章及法规为依据，建立有关数字图书馆信息资源安全的标准、规章及法律体系，对其信息资源进行有效的保护。

其次，要加强这些安全标准、规章及法律的执行力度，目前，国际上对计算机犯罪的打击力度正在加强，我国已制定了《中华人民共和国计算机信息系统安全保护条例》和一系列法律法规，并得到贯彻执行。数字图书馆实体应根据本单位的实际情况和具体的法律法规，加强执行力度，维护其信息资源的安全性。

数字图书馆信息资源服务与安全，不同于传统信息服务与权益保障，它是传统信息服务理论在信息化过程中的深化与拓展，是一种全新的信息服务理论与信息资源安全理论。TOR 模式旨在从数字图书馆的安全技术（包括安全的硬件软件系统的平台、适用的安全协议、安全机制、信息资源安全保障等），安全组织管理（包括权限管理、身份认证、数据库的维护、操作员管理、操作审计、安全检测），以及安全法规和政策等多个层面进行全方位的考虑，解决目前数字图书馆信息资源存在的安全问题。随着计算机技术与网络技术的发展，广大信息工作者和信息用户的安全意识的增强，以及相应的管理措施、法律、法规的出台，TOR 模式也会逐步发展变化并日趋完善。

## [参　考　文　献]

[1]　李海泉，李　健．计算机系统安全技术[M]．北京：人民邮电出版社，2001．

[2]　[美]匿　名．实用技术：Linux 安全最大化[M]．王　讽，路晓村，王景中，等译．北京：电子工业出版社，2000．

[3] 周朴雄. 基于 Linux 平台的主机入侵检测系统的研究与实现[D]. 武汉大学硕士学位论文, 2002, 5.
[4] 王志洪. 建立动态、实时、统一的计算机网络安全系统[J]. 电脑技术信息, 2000, (1).
[5] [美] 匿 名. 网络安全技术内幕[M]. 前导工作室译. 北京: 机械工业出版社, 1999.
[6] [美] Simson Garfinkel, Gene Spafford. 实用 UNIX 和 Internet 安全技术[M]. 王启智, 申功迈, 单和平, 等译. 北京: 电子工业出版社, 1999, (6).

(责任编辑 涂文迁)

# TOR Model to Solve Problems of Information Resource Security in Digital Library

**HU Chang-ping, ZHOU Pu-xiong**
(School of Information Management, Wuhan University, Wuhan 430072, Hubei, China)

**Biographies**: HU Chang-ping (1945-), male, Professor, School of Information Management, Wuhan University, majoring in information management; ZHOU Pu-xiong (1972-), male, Doctoral candidate, Information Management School, Wuhan University, majoring in information resource security.

**Abstract**: This paper introduces problems of information resource security in digital library, means and countermeasures to solve the problems in the world nowadays, and analyses the failure of these means and countermeasures. At last, we provide TOR model to solve the problems of information resourse security in digital library, and hope to do it wholly from three faces, including security technology, security organization and security regulation.

**Key words**: information resourse security; TOR model; digital library