医院信息化建设风险与数据安全管理

叶 萍

（南昌大学附属口腔医院 南昌 330006）

〔摘要〕 随着医院信息系统的发展和大规模应用，系统的安全性越来越受到重视。从系统级与应用级两个角度阐述如何增强信息的安全性，具体包括硬件设备安全、防病毒技术、客户机系统恢复、数据存储安全、数据库权限控制、数据加密及三级安全管理等措施。

〔关键词〕 存储安全；数据加密；系统安全；风险管理；身份认证

Risks in the Hospital Informatization Construction and the Data Safe Management *YE Ping, Dental Hospital Afliliated to Nanchang University, Nanchang 330006, China*

〔**Abstract**〕 With the development and the massive utilization, the security of hospital information systems are increasingly regarded as a vital issue. The paper depictes how to enhance the security ability from two aspects: system and application level, including hardware equipment security, antivirus technology, client computer system recovery, data storage safety, database authority control, data encryption and three – level security management measure, etc.

〔**Keywords**〕 Storage security; Data encryption; System security; Risk management; Identity authentication

随着医院信息化的发展，各种各样的应用越来越多，随之而来的医疗数据的安全性也越来越受到重视。医疗数据作为应用程序产生的结果，具有极为重要的价值。数据的安全性应该遵循 3 个原则：不得篡改，不能丢失，不能破坏[1]。系统必须针对这 3 个原则建立相应的机制。本文从系统级和应用级两个角度来说明如何增强信息数据的安全性。

1 系统级安全:保障系统正常运行

1.1 系统硬件设备

1.1.1 保障硬件设备安全的重要性 随着医院中信息系统及临床信息系统的大规模应用，系统提供越来越多的信息，一旦系统无法运行，不仅浪费时间，更重要的是大量的信息随着系统的瘫痪而无法读取，给医生治病救人带来了极大的不便。因此，保证硬件设备的安全运行，越来越为人所重视。

1.1.2 增设相同的设备及线路 一般来说，硬件设备最好的安全保障就是增设相同的设备及线路。对于数据库服务器来说，通常是采用双机热备加 RAID 5 + Hot Spare 的磁盘阵列柜。双机热备可以保证服务器硬件一旦损坏，将会在极短的时间内自动切换到另一台硬件中。而 RAID 5 + Hot Spare 的实现方式只是增加了一个热备份概念。当磁盘阵列中的一块硬盘出现故障，RAID 控制器会自动启用备份硬盘，并在几分钟之内，将数据写至新的硬盘之上。这样，就可以保证数据库服务器能够在极高的安全度下工作[2]。

1.1.3 供电线路多路备份 解决断电问题，机房最好采用双路供电的方式，一条线路从 UPS 引出，另一条线路从市电引出，两个电源分别接在不同的

〔修回日期〕 2010 – 02 – 24

〔作者简介〕 叶萍，高级经济师，发表论文数篇。

地方，即使其中一条线路出了故障，服务器及网络设备也照样能够正常运行，不至于因为电源问题而导致意外情况的发生。

1.1.4 应用服务器采用负载均衡 解决应用层故障，3 层构架的系统中，应用层的服务器采用 N + 1 台，并采用负载均衡机制，以保证当其中某台机器出现故障时，负载均衡器会自动将应用负载到其他的应用服务器中，以达到 24 小时不停机的效果。

1.1.5 采用双网卡相互监测 主网卡工作时，备用网卡并不工作，只是负责监测主网卡工作情况。当备用网卡发现主网卡出现了故障（断线、包之间传输有错误）时，就会自动将主网卡断掉，并在几秒内接管主网卡的工作。

1.1.6 交换机双机网络级容错方法 当系统检测到某台交换机的负载过重时，会自动根据交换机均衡负载的算法将一台交换机上的工作转换到另一台交换机上去，从而在保障高可靠性的同时保证了高效率。

1.1.7 增设辅服务器 有两种方式，一种是采用 N + 1 台数据库服务器，平时所有运行中的数据备份的一份将会存储在该台辅服务器中。如果某台服务器出现问题，就立刻将数据备份在该台辅服务器中启用。另一种是采用服务器镜像，数据写到主服务器的同时还写到了辅服务器上，通过锁定服务器数据保持了数据的完整性。一旦主服务器出现问题，可以快速切换到辅服务器上。

1.1.8 增加异地备份 使用光纤或高速以太网，定时将数据库中的数据进行异地备份，以备不测。异地的最低要求是不同楼层之间，最好是在两栋楼之间。异地备份要求可以长期保存。

1.2 防火墙、防病毒技术及客户机系统恢复

1.2.1 防火墙及防病毒技术 由于病毒的主要传播途径已由过去的软盘、光盘等存储介质变成了网络，同时也为了防止黑客通过网络袭击医院的内部网，因此，内部网和公众网必须通过硬件防火墙来连接，而不能直接进行连接。这样，可以有效地防止外部攻击，保护内部网络的正常运行。同时需要部署网络版的杀毒软件，以对整个网络实行全方位、多层次的病毒防护。取消网络中所有的共享资源，对必须共享的最好设置为只读、加密访问、控制访问权限等[3]。

1.2.2 客户机系统恢复 在医院会有上百个客户机在运行，而每台客户工作机上运行着大量的软件，一旦客户机出现问题，将会导致系统的某些节点无法正常工作，阻塞流程，也一样会造成很严重的后果。因此，如何有效地保护客户机就成为重要的工作。首先，在各终端所在地，常备一台以上的备用机器。一旦出现无法立刻恢复的问题，可以用备用机器代替原工作机。其次要使用 ghost 软件，一旦出现问题，运行 ghost 即可“克隆”出原机器的全套配置。有条件的单位还可以通过在客户机中安装还原卡提供对系统盘的还原保护。这样整个系统的安全得到有效的保障。

2 应用级安全:保障数据的安全

2.1 数据存储安全

具备数据备份功能，包括自动定时备份、程序操作备份和手工操作备份。为应对不可预见的事故及灾害，数据必须异地备份。虽然磁盘阵列和双机热备份技术已经形成了数据冗余，但不能代替离线备份，有必要制定安全可靠的备份计划。将隔年的数据转储到备份数据库或磁盘、光盘，避免人为操作、硬盘损坏、病毒及黑客造成关键数据的永久丢失，保证数据的可用性、一致性和完整性。

2.2 数据库权限控制

2.2.1 权限管理库 首先用公用连接信息登录到权限管理库中，再通过权限库中的加密信息得到登录用户数据库的用户名与密码，并由程序自动连接到用户数据库中。这样可以保证黑客无法得到登录用户数据库的用户名和密码。同时，由于权限相关信息都为加密保存，即使非法用户能够登录该权限管理库，也无法修改表中的数据。同时，用户数据库的登录密码应该定期进行更换，密码长度保持在 8 位以上，必须包含数字与特殊字符[4]。

2.2.2 用户数据库 为了防止用户数据库的数据

被破坏，管理人员还应该将所有数据库中不必要用户全部锁定，只留下正常的登录用户以及系统管理员用户。系统管理员用户的密码也应该定期更换，密码中也必须包含数字与特殊字符。尽量保证各个工作站除了唯一登录程序以外，无法利用其他程序连接数据库。

2.3 电子身份证明及 3 级安全管理

2.3.1 电子身份证明 医生的登录名、密码及个人电子签名等信息保存在类似于 U 盘的加密存储设备中。用户在登录系统时，必须将该类设备连接在计算机中。由程序读取加密存储的用户登录信息，同时在登录时应该增加随机的校验码输入。程序在运行时，该设备需要一直连接在计算机中。如果该设备从计算机中拿下，该程序必须进入锁定状态或者退出。

2.3.2 3 级安全管理 由住院医师填写的病程记录等内容，必须提交上级主治医师批阅，原住院医师不可更改提交后的记录，除非由主治医师退回。主治医师批阅后的病程记录必须提交上级主任医师批阅，如有问题，可以退回主治医师修改。所有的记录都必须保留修改痕迹，正常文书可以只显示最后一次修改后的样式，但是相关医师及审计部门可以查看该记录所有的修改过程，修改的内容以特别的方式来显示。

2.4 数据加密

为了保证数据在传输过程中不被篡改，还必须要注意数据的传输方式。所有的数据都是以小数据包的方式在网络中进行传输，最终存储到数据库服务器中。不论 3 层构架还是两层构架的应用程序，数据在网络中传输时一般都是采用明码的方式。这种方式下，黑客采用截获数据包的方式可以知道数据包的内容，并可以进行篡改。这是一个很大的隐患，一旦被人利用后果不堪设想。

要去除这种隐患，必须要采用数据加密技术。两层构架的程序，因为是采用数据库连接，所以在应用程序到数据库之间需要采用数据库的传输加密，这种模式一般的数据库都会提供。而在 3 层构架中主要考虑的是客户端到应用服务器之间的加密方式，一般来说，应用服务器会采用 HTTPS（超文本安全传输协议）来建立一个加密连接。当浏览器要与远端 Web 服务器建立安全连接时，自动使用 SSL（安全套接字层）加密算法进行加密。但是由于美国政府禁止 40 位以上的加密算法出口，多数流行的应用服务器软件国际版本只支持 40 位以下的弱加密算法。因此对于要求强加密的数据传输，需要采用 SSL 安全代理软件再进行一次 128 位的加密。具体方式为：当浏览器要与远端 Web 服务器建立安全连接时，向安全代理发出请求，由安全代理负责与远端 Web 服务器建立连接。连接建立后，浏览器与服务器之间的数据传输是经过安全代理转发完成的。浏览器与安全代理之间的数据传输是用浏览器本身支持的 40 位以下的弱加密算法加密的，而安全代理与远端 Web 服务器之间的数据传输则是用高强度的数据加密算法加密的。

3 结语

总之，医院信息化建设安全管理不是一劳永逸的，在遵循不得篡改、不能丢失、不能破坏的 3 个原则下，信息科、医院管理层时时刻刻要讲、要管、要做。管理人员和操作人员必须共同努力，因此医院在加强系统级和应用级管理的同时还需要不断提高操作人员的风险与安全意识，齐抓共管以确保医院信息系统安全可靠运行。

参考文献

1 任俭. 医院信息安全〔J〕. 中国卫生信息管理杂志，2006，(3)：25－26.

2 Aiken@ Club. 磁盘阵列技术原理分析〔EB/OL〕.〔2008－07－25〕. http：//www. dostor. com.

3 李包罗. 医院信息安全矛盾尖锐化〔EB/OL〕.〔2009－04－12〕. http：//industry. ccidnet. com/art/12129/20090412/1737155－1 html.

4 SSL 原理解密〔EB/OL〕.〔2006－04－26〕. http：//www. yesky. com.