医院网络安全现状分析及研究

The analysis and research of network security situation in hospital

张震江　（中国人民解放军总医院计算机室 北京 100853）

摘要：医院网络安全一直是医院信息化的长期话题，本文总结了作者多年来网络管理的经验，系统地阐述了诸如网络设备可靠性、计算机病毒及非法入侵、内网安全、雷击和人为因素等威胁医院网络安全的因子，并提出了相应的防范措施，对于医院和医疗机构建立新的网络或者对现有网络进行改造都具有一定的理论指导意义。

关键词：医院　网络安全　信息安全

网络是现代医疗信息的载体，网络建设是医院信息化的一个重要组成部分，网络性能的好坏直接关系医疗工作的正常与否。在医疗信息日益膨胀的今天，网络的重要性变得更加突出，面对越来越庞大的医院网络，越来越多的网络管理人员认识到，提升医院网络安全性已经迫在眉睫。

1　医院网络安全性分析

1.1　医院网络现状

同过去相比，医院网络的状况有很大不同。十年前，医院信息系统（HIS）刚刚得到比较系统的应用，医院网络规模小，信息点数量少，医疗信息量少，用户群计算机水平不高，网络管理相对容易。

随着芯片技术和计算机技术的发展，医院网络架构从一个冲突域的局域网逐渐过渡到三层的交换网络，可管理网络设备为网管人员提供了便利，布线工程走向标准化和正规化，现在一栋楼里的信息点数量相当于以前整个医院的信息点数量，网络的触角从最初的临床科室延伸到了非临床科室以及与医疗工作相关的所有层面，医院信息化从不成熟到不断改进，许多大型应用如 PACS（Picture Archiving and Communication Systems 医学影像存档与通讯系统）、办公自动化等都已经得到成功应用。医院的网络如同一个巨大的工厂，承载着大量数据每天 24 小时不间断的运转着。

以中国人民解放军总医院为例，据统计，2005 年全院维护总量为 5844 次（见图 1），其中有关网络的故障维护量为 884 次，但从统计数据上看所占比例并不很大，但是从网络的特性和重要性来看，由于网络互连，一旦出现故障，影响的往往是一片区域，因此这个数字已经相当值得关注。

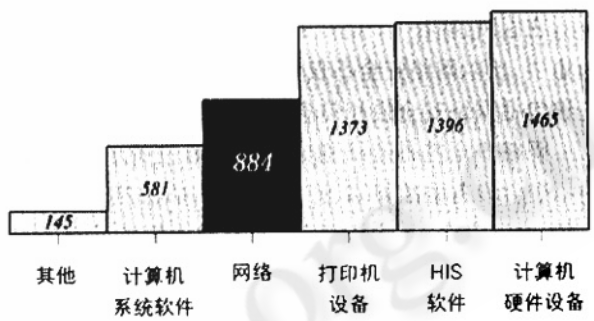

图 1　2005 年解放军总医院计算机室维护量统计

1.2　主要数据流及其特点

由于医院里绝大多数业务都已经实现信息化管理，数据最终都要存入数据库，所以医院网络所承载的主要是医疗信息数据，其特点是：

（1）对于网络稳定性要求高。医院里一天 24 小时随时都可能有病人前来就诊，病人信息和医疗信息都要保存在计算机中，从门诊挂号到住院都离不开计算机的正常工作，所以网络要相当稳定。

（2）对于网络安全性要求高。存储在数据库中的数据对于医院和病人都很重要，这些数据必须能够安全、及时、准确的通过网络保存到数据库中，同样也必须能够安全、及时、准确的通过网络从数据库中读取出来，病人信息的私密性较强，对网络安全性的要求也就

较高。

(3) 网络上的数据流量分布不均衡,具体表现在以下几个方面:

① 从时间上看,网络流量分布不均衡。据统计,周一至周五工作日期间,每天上午 9:00 ~ 10:30 以及下午 16:00 ~ 16:30 为网络繁忙阶段,具体表现为数据存取时间相对较长,部分应用程序频繁死锁;其它时间网络状况良好。

② 从空间上看,网络流量分布同样不均衡。门诊集中了挂号、收费、医学图像等数据的存取,数据流量最大,病房内数据量相对较少,其它部门的数据量最少。

③ 从业务上看,有关图像的 HIS 系统应用数据流量较大,其它 HIS 系统应用虽然频繁,但是每次与数据库交互的数据量都不大。

1.3 网络安全性分析

在医院这样一个特定的领域内,各种医疗数据最为重要,所以网络安全不仅仅指传统意义上的概念,而应该包括网络安全性和信息安全性。

网络安全性是网络稳定性和可靠性的前提保障,包括硬件设备的故障率、计算机病毒、非法流量和非法入侵、内网安全、人为因素等,都会成为影响网络安全的重要原因。这些因子产生的危害程度和后果各不相同,但是都对网络的正常运转构成威胁,影响了数据的可用性和完整性。

信息安全性是医院信息化建设不可缺少的组成部分,主要包括两个方面:一是基于系统的数据安全性,即存储安全,如何使服务器在硬件故障甚至是灾难性故障的情况下使数据的丢失减少到最小限度[1];二是基于网络的数据安全性,如何使各工作站的工作人员不论是误操作还是恶意攻击,对服务器的数据造成破坏减低到最小限度。

目前,医院管理人员对网络和信息的安全意识还不够高,采取的防范措施也不完善,安全隐患随处可见,有些程度非常严重。例如,对医院信息点的管理,为了方便和满足日后扩充的需要,建网时设计人员一般都会考虑布点数量尽可能多,布点范围尽可能广,甚至将某些信息点设置在公共场合,如门诊大厅(用于导医触摸屏计算机),这就是一个安全隐患。试想如果有人拿着手提电脑在门诊大厅通过该信息点接入医院网络,利用在互联网上就可以轻易找到的黑客软件和嗅探工具就可以对医院网络的状况掌握的一清二楚并发起攻击,其后果不堪设想,患者和医院将遭受不可弥补的损失。

2 影响网络安全性的因子及防范措施

2.1 保障硬件设备可靠性

网络硬件设备包括交换机、各种线缆、连接模块以及网卡等,其中有些硬件设备属于精密设备,环境对设备寿命影响很大,而且本身具有使用年限。解放军总医院共有交换设备近 200 台,其中有部分设备使用时间已经超过 5 年,2005 年度更换在用交换设备共计 11 台次,具体统计结果如表 1 所示。

表 1　2005 年解放军总医院计算机室网络故障统计

故障类别	故障次数	说明
交换机	16	更换 11 台次
双绞线	12	其中 2 次因为装修施工扯断
小型集线器(HUB)	11	更换 9 台次
RJ45 模块	5	
网卡	5	更换 5 块
光电转换器	2	
光纤	1	

对于分布在整个医院院区的网络设备,应该建立完善的巡查制度,主要包括以下两种方式:

(1) 通过软件进行网络监控。主要包括网络链路状态监控和设备状态监控。

(2) 现场巡查。主要包括配线间温度、湿度、灰尘度巡查,设备温度、端口指示灯状态巡查,供电电源状态巡查等。

不论哪种方式,都应该指定专人负责,定期做记录。实践表明,交换设备的故障 80% 以上都是由于温度过高所导致,温度过高的最主要原因是风扇故障,而风扇故障最主要的原因是久积的灰尘。通过用手触摸交换机,可以感受到温度和风扇强度,由此可以初步判断交换机工作状态正常与否。通过巡查可以提前预测到设备可能出现的故障。目前解放军总医院计算机室的工作人员每周巡查一次全网设备,并不定期通过网管软件观测网络状态。

2.2 计算机病毒

计算机病毒破坏性强，作用范围广，有人已将其列为未来社会的公害。网络的发展更加速了计算机病毒的传播。目前网络上流行的病毒大多以损耗系统资源为特征，其中以蠕虫病毒的危害性最大，对医院网络的威胁也最大。通常情况，医院信息网络属于内部局域网，尤其是某些部队医院，与互联网之间是物理隔断的，那么病毒从何而来？杀毒要除根，除根要寻本。归纳来说，医院网络中的病毒来源主要有以下几个：

（1）安装配发计算机时感染病毒。

（2）内网外联感染病毒。

（3）使用盗版软件和光盘感染病毒。

（4）用户使用移动介质引入病毒。

针对上述病毒来源，医院原有的病毒防范措施已是捉襟见肘（比如在 BIOS 中将软驱封掉，配发的计算机一律不安装光驱等），随着医院信息化的发展，远程医疗、PACS 的技术日趋成熟，医疗信息的整合是大势所趋，未来的医院网络必将并入到互联网，因为只有这样才更有利于医学的发展，才更有利于提高全民健康水平。鉴于此种考虑，医院应从各个方面主动积极地抵御病毒入侵，采取有效的防范措施，具体包括：

（1）制定严格的规章制度，从管理层面上把关。比如配发的工作用计算机一旦被发现安装了游戏或其他非常规软件，则扣除该单位经济效益考评分。

（2）通过有效宣传，提高全院人员防范病毒的意识。

（3）客户端计算机安装防病毒和防火墙软件，并定期升级。

（4）完善数据库备份方案，保证备份数据不被病毒感染。

（5）连接互联网的入口处设置硬件防火墙和 IDS、IPS 设备。

（6）积极观察网络异常流量，发现有病毒迹象及时查找源头并清除病毒。

至于将来医院网络并入到互联网以后，可能要对医疗资源的共享等级进行的相应划分，不在本文的讨论范围。

2.3 内网信息安全

越来越多从事 HIS 工作的管理人员意识到，更大的威胁可能会来自于网络内部。医疗信息尤其是患者的医疗信息私密性较强，而网络内部总会有一部分用户对这些信息拥有较大的处置权限，可以随时随地对数据库记录进行增删改。如果不能以有效方式加以控制和约束，就会造成统计数据不准、医患纠纷频繁等严重后果。而造成这种后果的直接原因就是网络管理上的漏洞和系统设计上的缺陷。

目前，部队医院广泛使用的“军卫一号”HIS 系统，采用的是 Oracle 自身的 RBAC 访问控制机制，即基于角色的访问控制机制，现在看来是存在安全隐患的。有的管理员发现，尽管 Oracle 数据库软件本身的安全性很高，但是登录 Oracle 的用户可以直接对数据库进行操作[1]。因此用户只要简单的掌握 SQL Plus 工具的用法以及 SQL 语句，就可以通过 SQL Plus 对权限内的表数据进行增删改操作，从而脱离了应用程序中所做的各种限制，大大增加了安全隐患。

据研究，目前医院内网的安全漏洞及相应防范措施有：

（1）信息访问控制机制存在严重漏洞，企图依靠用户的“愚昧”来保证数据的安全性是不会维持多久的，应该立即寻求新的机制进行数据访问控制。

（2）切实执行规章制度，不要把规章制度变成一纸空文，一个安全的网络 80% 依靠制度上的管理，剩下的 20% 才是需要靠技术去解决的。

（3）禁止使用 DHCP 机制，尽量固定分配 IP，并记录日志，密切注意非法 IP 及其流量。

（4）对于数据库的重要操作做系统日志，做到有据可查，日志要建立完善的备份方案。考虑到日志文件的大小限制，可以适当调整写日志策略。

（5）暂时用不到的信息点，应该将设备端口状态置为 Disable，医院药品要求管理到“片”，网络应该要求管理到“点”。

（6）医疗信息应该经过加密后再通过网络保存到数据库中，防止被恶意侦听，但是目前要做到这一点还很困难，因为医疗信息是要被共享的，这是一个矛盾，期待以后的技术能够解决。

2.4 防雷击及人为因素

2.4.1 防雷

防雷击已不是新鲜概念，但由于不能引起足够的重视，也成为网络的重大安全隐患。如果防护不到位，就有可能造成人员伤亡和财产损失。雷击多发地带的

（下转第 93 页）

(上接第 89 页)

防雷击措施一般都比较好,所以相对来说,雷击少发地带更加需要引起重视。

2.4.2 人为因素

应该采取必要的措施降低人为因素导致的网络故障率。具体措施包括:

(1) 尽量不要在临床科室使用带电源适配器的小型集线器(HUB)。这也是局部网络极不稳定的重要原因,有时维护人员要反复到现场数次解决此类问题。

(2) 施工前加强施工单位与网络维护人员的协调,断电前制定详细的切换方案和应急方案。

(3) 合理规划配线间和机柜位置,远离人群,避免噪音。

(4) 分置配线间内的强电电源和断电频繁的照明电,争取单独供电,和供电部门协调保证 24 小时不断电。

(5) 另外还有一些不可预见的人为因素要注意随时观察,尽量避免因此产生的网络故障。

3 结语

医院网络安全性将是医院信息化的一个长期话题,上述影响医院网络安全性的各个因素和防范措施都是在长期工作中总结出来的经验。可以预见,未来的医院网络将更加复杂,摆在网络管理员面前的将是更加严峻的考验。

参考文献

1 孙剑, 医院管理信息系统的安全机制[J], 石家庄白求恩医学院学报,2003.9. 182-184。

2 傅征、任连仲编著, 医院信息系统建设与应用[M], 北京 人民军医出版社,2002. 167。

3 James Trulove 著,沈鑫剡译, 局域网布线[M], 北京 人民邮电出版社, 2002.2. 45-52。