医院信息系统安全分析与管理

赵 爽

（常州市第一人民医院 常州 213003）

〔摘要〕 阐述医院信息系统安全工作应注重的几个方面，包括机房环境、网络和服务器安全、容灾备份、终端管理、病毒防护及信息系统安全管理制度，就其具体措施提出建议。

〔关键词〕 医院信息系统；系统安全；网络安全

〔中图分类号〕R－056 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2018.11.007

Security Analysis and Management of Hospital Information System *ZHAO Shuang, The First People's Hospital of Changzhou, Changzhou 213003, China*

〔**Abstract**〕 The paper elaborates on the multiple aspects that shall be focused on in the security practice of Hospital Information System (HIS), including environment of the plant room, security of the network and the server, anti－disaster backup, terminal management, virus protection and the information system security management regulations, and puts forward suggestions on the specific measures.

〔**Keywords**〕 Hospital Information System (HIS); system security; network security

1 引言

医院信息系统安全管理并不是一个单一的项目，是一项系统工程，针对信息系统的不同环节应有不同的规划与设计。医院信息系统安全管理是保证信息系统的高可用性、完整性、机密性以及所有相关资产的一项体系制度。单位管理层及信息科、总务科、基建科等相关部门必须积极主动参与到信息系统安全管理建设中。医院信息系统安全管理包括多个方面的内容，如机房、网络和服务器安全以及信息系统安全管理制度、容灾备份、防病毒、终端桌面管理等。其中任何环节出现问题都会给医院信息系统安全带来不稳定因素，影响医院正常诊疗工作，甚至会对医院的信息系统造成损害。

2 机房环境安全

2.1 概述

核心机房作为承载医院信息系统的核心枢纽，是整个信息系统的基石，机房用于系统运行、存储数据等，安全、高效的运行可以保障系统和网络的安全，因此机房安全必须引起足够的重视，其中机房供电、温湿度控制、消防安全为重中之重。

2.2 机房供电

机房使用不间断电源（Uninterrupted Power Supply，UPS）供电并保证 UPS 运行正常。将市电引入到 UPS 上可以为设备提供电力，由于 UPS 具有稳压的作用，还可避免因市电电压不稳造成对设备的损伤。

〔修回日期〕 2018－06－06

〔作者简介〕 赵爽，工程师，发表论文 2 篇。

2.3 温湿度控制

选择精密空调来精确控制机房温湿度。服务器、交换机等设备对温湿度有着较高的要求，温度偏高影响电路的稳定性和可靠性，元器件易损坏，机房温度控制在 23℃ ±1℃较为适宜。湿度过高易造成电路短路，湿度太低易引起静电效应，威胁设备的安全，机房湿度控制在 40% RH ~55% RH 之间较为适宜[1]。

2.4 消防安全

机房消防措施按照国家数据中心机房 A 级标准设计，主机房必须配备烟感、温湿感报警装置和七氟丙烷气体灭火装置两部分。此外在主机房内应具备双电源（交流电与直流电）应急灯、院内消防应急处置电话、火灾一键报警按钮等消防设施。

3 网络安全

3.1 架构安全

3.1.1 概述 医院内部局域网应用繁多、交互广泛，网络架构的设计要考虑物理环境、业务类型、设备配置、边界联网方式、网络维护管理等因素[2]。在构建内部局域网时通常将医院整体网络划分成 3 层拓扑：核心层、汇聚层、接入层。这种 3 层网络结构清晰，实现冗余性，提升安全性、可靠性，易于维护管理并具备良好的扩展性。

3.1.2 核心层 用于高速转发整个网络数据流量，不对数据包做任何操作。作为网络汇聚的枢纽集中着所有汇聚层设备需要交换的数据，必须具有高效的数据转发和处理能力。因为核心层是整个网络的中心，必须要采用双机冗余热备或者虚拟化来提高网络性能和冗余性。

3.1.3 汇聚层 位于核心层与接入层之间，用于汇聚各自接入层交换机，在终端接入核心层之前先做汇聚，通过访问策略控制不同网段间的通信访问，将通过策略匹配的数据传输至核心层，减少核心层的压力。汇聚层是接入层的汇聚点，能够提供路由决策，实现安全过滤、流量控制、接入控制等功能，因此汇聚层交换机所需性能在核心层与接入层之间。应选用具备高速转发能力的 3 层交换机。

3.1.4 接入层 主要是将设备连接至网络并提供相应的网段间通信服务。接入层设备应采用低成本、高端口密度、只有基础转发功能的 2 层交换机。

3.1.5 链路 在构建医院网络时还应考虑链路冗余性，为网络拓扑结构的每一层的每台交换机与下一层的每台交换机之间有两条链路互连，启用交换机的生成树协议（Spaning Tree Protocol，STP）防止多条路径之间可能导致的网络环路，也可在路由器接口上启用热备份路由器协议（Hot Standby Router Protocol，HSRP）实现备份路由器在主路由器失效时的接替工作，即使某台交换机路由器在工作中出现故障，相连的其他设备会调整选择其他正常的备用设备与可达路径，保持数据间的正常转发与路由，使网络保持畅通。在网络架构优化方面，可将接入层交换机端口配置为快速端口（PortFast）模式，在核心层到汇聚层再到接入层之间使用链路聚合，将多条物理链路组捆绑成一条具有更高带宽的逻辑链路，使链路具有负载均衡功能，提高整个网络的传输效率、吞吐量和安全性。

3.2 应用安全

3.2.1 概述 随着医疗服务对于互联网技术的广泛应用，各不同部门的工作业务、管理业务和科研需求都离不开互联网访问。互联网不仅使医院网络的数据流量激增，同时非法侵入的可能性也大大提高。为保护医院信息系统安全，需对内、外网络的访问、数据信息的读写等加以控制和保护，避免信息系统遭受病毒及木马的入侵，防御来自互联网的网络攻击和威胁，抵御网络黑客的攻击和勒索破坏[3]。网络安全拓扑，见图 1。

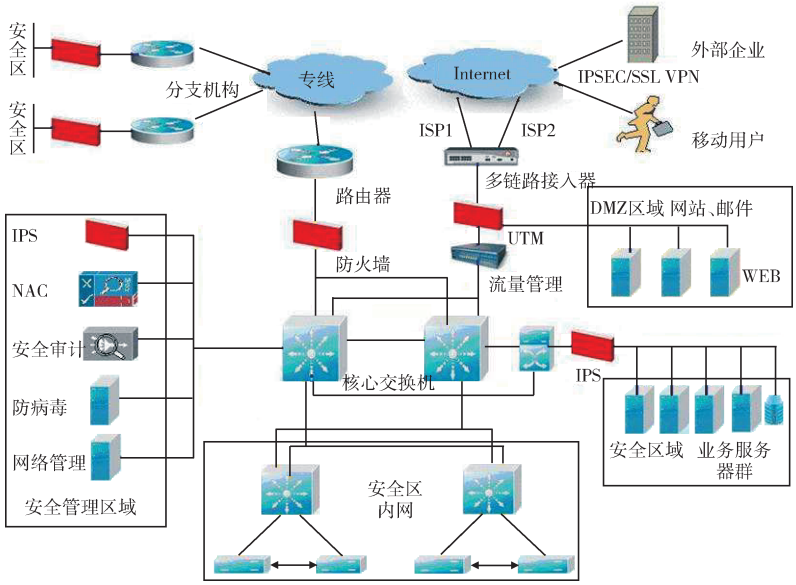

图 1 医院信息系统网络安全拓扑

3.2.2 内外网络隔离 医院网络体系结构由 3 个区域组成：内部网络、外部网络及边界出口网络。内部网络与外部网络之间使用网闸完成数据交互及隔离，此外严格控制内外网之间出现其他数据入口和出口。在外网及边界网络区域都部署防火墙，避免医院网络受到外界的攻击，为受信任的用户配置应有的最小访问权限，规范内部用户的可执行操作，防止外部用户访问内部网络。

3.2.3 内网访问控制 利用虚拟局域网（Virtual Local Area Network，VLAN）及其之间的路由技术来实现对内部子网的逻辑隔离与延伸。按照医院部门、功能、楼层不同划分出若干 VLAN，实现内部子网的隔离，便于网络工程师管理，确保各个子网数据的安全。VLAN 间的隔离将网络整体的大型广播域分割成一个个互不干涉的小型独立域，保障整个网络不受个别子网影响。通过在内网架设 Radius 服务器，接入层交换机开启 802.1x 协议，可以限制未认证终端设备通过接入端口访问网络，未认证的终端设备将被放置在无网络的隔离 VLAN 中，只有通过认证的终端设备才能被放进业务 VLAN 网段。

3.2.4 网络安全检测与防御 防火墙截获数据包，按照配置的规则对数据包的源地址、目的地址、源端口、目的端口来判断是否放行[4]。入侵检测（Intrusion Detection System，IDS）、入侵防御系统（Intrusion Prevention System，IPS）和防毒墙被视作防火墙之后的第 2 道防护措施。IDS 是一种监测系统，一般以旁路方式部署，实时监控并自动检测网络系统是否遇到非法入侵，记录并分析各种异常行为，进行相应的入侵规则匹配，在识别入侵攻击的特征后向控制台报警并提供防御记录，随后及时将入侵事件反馈给网络管理员。IPS 是一种主动防御系统，一般部署在防火墙后方，可深入网络数据的内部，感知并检测流经的数据，对照数据之间的正常关系来识别可疑行为，检测到异常特征后及时对进入网络的恶意代码进行丢弃以阻断攻击，即时阻止木马病毒的蔓延。通常将防火墙、IDS、IPS、防毒墙等安全设备结合部署，实现针对医院信息系统的入侵检测、防御、阻断为一体的综合性安全防护体系。

4 服务器安全

服务器是医院信息系统的关键，为保证业务系统平稳、不间断的运行，信息系统使用两台高性能服务器和两台高速存储，通过赛门铁克 VCS（Symantec Veritas Cluster Server）构建双机热备磁盘阵列模式，俗称“2+2”模式，见图 2。医院信息系统（Hospital Information System，HIS）和检验信息系统（Laboratory Information System，LIS）分别在

两台服务器上同时运行，当主服务器发生故障时备用服务器通过 Veritas 群集自动切换，将核心业务快速切换从而保证信息系统的持续性，提高系统的可用性。服务器应配有专业的系统管理员来管理，有规律地更换登录密码，密码严禁向任何人泄露。服务器管理专员应每日对服务器的系统、安全和应用日志以及关键系统文件、运行负载及状态等进行巡检并记录成文档，形成完整的巡检资料台账[5]。

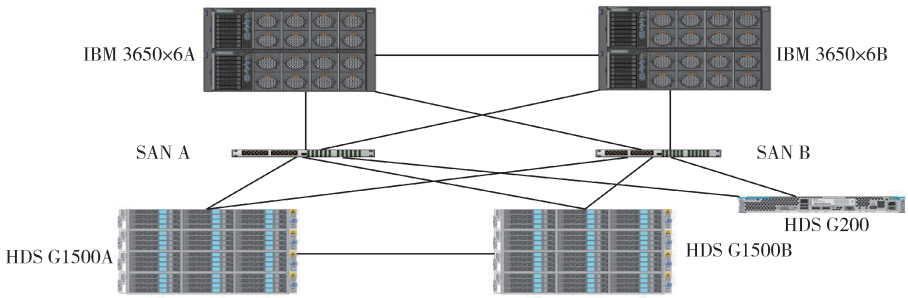

图 2 医院信息系统服务器存储拓扑

5 容灾备份

尽管信息系统规划、设计、实施、维护合理，安全性较高，故障的发生都无法避免，因此备份容灾方案必不可少。常州市第一人民医院建有多个异地容灾机房，均配置容灾服务器及存储，通过存储远程镜像，将核心机房的业务数据同步到异地容灾机房，保证异地数据与核心业务服务器数据同步。当核心机房发生灾难性故障，业务系统能迅速在容灾机房的服务器上部署，终端业务保持不间断，大大提高业务的高可用性、连续性和安全性。

6 终端管理

终端是用户进入信息系统的接入点，越是靠近用户往往就越有风险，对终端安全疏于管理会造成数据的泄露或损坏。医院所有内网终端都拆除光驱并将 USB 存储禁用，在内网架设域控制器，所有客户端在域控管理下只能使用业务程序，终端都部署桌面管理系统，可实时监控网络行为、操作系统下的各种行为并进行审计，通过系统保护、非法外联、进程保护等功能限制用户通过终端对信息系统进行违规操作。桌面管理系统还具有固定资产设备管理功能，对硬件设备的变更进行提示、告警、审计。通过开启客户端操作系统内 802.1x 认证功能，只有通过认证的客户端才能与内网通讯，防止非法客户端进入内网。

7 病毒防护

随着互联网技术的发展，系统信息化程度的迅速提高，病毒破坏力更强、传播性更快、传播范围更大（如勒索病毒），对信息系统构成更大的威胁，对此医院应用以下 3 种防范措施：一是为提高职工计算机、网络安全意识，开展安全应用知识培训并在企业微信推送相关病毒防范知识。二是在内网服务器、终端均部署正版网络版反病毒系统以及防火墙、IPS、AV 等安全设备，网络版反病毒系统定期更新扫描引擎和病毒库、扫描查杀，做好升级、维护记录。三是加强终端管理，采取域控组策略控制用户可用操作，IP 与 MAC 地址绑定，终端卸除光驱，禁用通过 USB 接入的一切存储外设等方法来对内网安全进行保护。

8 信息系统安全管理制度

要保证信息系统的安全，仅通过技术手段进行防范是不够的，还必须针对系统的各个环节建立完

（下转第 44 页）

4 结语

本文主要介绍医护通服务平台的设计及实现，使平板电脑作为移动智能终端设备应用于病床发挥出移动医疗的优势。平板电脑的部署以及相关服务平台的实施有助于更加深入了解移动医疗行业这一新领域的价值，借助其服务平台使医务工作者的管理变得更加科学、有效。提高医生和护士工作效率的同时使患者更加了解自身疾病以及医学知识，改善患者住院体验，提高满意度。下一步将在服务平台基础上做进一步扩展，如增加患者缴费、手术提醒、服药提醒、视频点播、游戏对接等多种功能，满足患者在住院期间的医疗、服务、娱乐全方位需求。

参考文献

1 刘伟，邓建强. 基于 .NET 的医院信息仿真实验系统的设计与实现［J］. 中国数字医学，2013，8（11）：28－30，42.
2 邹代坤. 基于移动智能终端的医疗服务系统设计与实现［D］. 武汉：武汉科技大学，2015.
3 张虎军，李运明，谭映军，等. 移动医疗技术现状及未来发展趋势研究［J］. 医疗卫生装备，2015，36（7）：102－105.
4 彭晓娜，张宇红. 移动医疗产品服务系统设计探究［J］. 包装工程，2013，34（20）：77－80，87.
5 刘伟，陈鹤年，张锦，等. 医院信息系统课程教学体系改革探讨［J］. 医学信息学杂志，2013，34（10）：86－89.
6 李威，刘伟. 住院管理仿真子系统床位管理模块设计与实现［J］. 软件导刊，2016，15（4）：126－128.
7 傅剑飞，刘伟. 住院管理仿真子系统医嘱管理模块设计与实现［J］. 软件导刊，2016，15（5）：94－96.

（上接第 35 页）

善的信息系统安全管理制度。完善的管理制度是保障信息系统安全、可靠、稳定运行的重要因素，所以要根据医院内部实际情况来制定信息安全相关规章制度并落实到实处。完善的信息系统安全管理制度应包含针对各种可能的突发情况制定的应急处置方案，对信息系统维护人员的系统权限应分类分级设置，按分工、管理等级不同来对应不同组别的用户组权限。定期组织相关部门进行演练以确保信息系统在出现故障情况下能快速恢复业务。软件部门对信息系统软件参数的修改、存储过程维护、程序修改、数据库维护等应有相关流程对其进行严格管控并留有记录，最终形成台账。

9 结语

医院信息化建设与安全管理工作是艰巨、复杂和长期的过程，这是由目前医疗行业信息化所面临的客观条件决定的。随着医疗行业信息化建设覆盖面越来越广，计算机、网络信息技术高速发展，也将面临更多的挑战。完善信息化安全相关工作，共同推动医院信息化建设安全、可靠、稳步向前发展。

参考文献

1 李楠. 卫生网络和信息安全的现状分析［J］. 中国软科学，2015（2）：96－97.
2 贾铁军. 网络安全管理及实用技术［M］. 北京：机械工业出版社，2010：322.
3 李领治，杨哲，纪其进. 实用计算机网络教程［M］. 北京：清华大学出版社，2017：297.
4 贾铁军. 网络安全管理及实用技术［M］. 北京：机械工业出版社，2010：10.
5 薛颖. 试析医院计算机网络安全维护［J］. 科技展望，2014（15）：23.