3.3 预约提醒 预约提醒是对就诊者的提醒，分为两个方面：(1)在预约时间、挂号级别和医师都没有发生改变的情况下，提前 1 d 通知患者按时就医，并显示就医的大概时间段[6]；(2)预约的医师在预约当天不能出诊或有改动的，将短信通知已经预约此医师的患者，由患者来选择修改预约时间或退号。

3.4 无卡预约 打破了患者必须有医院患者标识(ID)号的局限，即使患者从来未在医院进行过身份主索引的建立，也可以通过无卡预约方式进行预约，就诊时再进行身份信息的补登。

3.5 实名制预约 在预约挂号时录入身份证号，此时身份证号和患者 ID 号一一对应，这样可以保证数据的惟一性[7]，即便患者忘记了患者 ID 号也可以通过身份证找回，同时取号时通过身份证进行验证，有效避免了“倒号”现象的发生。

3.6 多样的用户识别取号 预约用户按预约时间到达医院，在自助取号机上通过刷二代身份证、医院就医卡、医保卡、城市一卡通或输入用户名密码方式，自动取号[8]。

3.7 多种预约方式、支付方式、退号方式实现交叉灵活运用 患者数据统一保存在“医事通”平台预约诊疗数据库中，支持预约方式、支付方式、取号方式等不同方式的灵活使用。如网上预约成功后手机退号、手机预约成功后网上退号、现场预约手机退号等。

3.8 自助终端机服务 现场预约方式(院前自助机)是在医院门诊大厅配置多台自助设备[9]，患者可直接在此设备上进行患者注册、挂号查询、预约退号、预约挂号、缴费、化验单查询、发票打印、病历查询等服务。目前支持的方式有城市一卡通、二代身份证等方式。

4 应用效果和思考

新一代预约挂号系统的开发是医院依托预约诊疗服务平台实施业务流程再造，优化患者就医程序的一项重要举措，取得了预期的成效，但仍然存在局限性，尚需在不断摸索中对系统进一步完善。

4.1 应用效果 (1) 进一步缓解挂号难状况：利用该预约挂号系统，用户就可以通过 Internet 网络、手机、自助终端机等多种预约方式和多种支付方式，灵活方便地预约到医院的专家、专科号，感受到预约服务的“方便、灵活、省时、省力、省钱”。(2)进一步改善门诊就诊秩序：它能帮助医院更好的改善就医环境，简化就医环节，缩短就诊时间，提高医疗服务质量和效率，合理调配医疗资源，建立和谐医患关系，从而真正体现了以患者为中心，一切从方便患者出发，符合当今医院人性化温馨服务的理念。

4.2 思考 (1) 加强监管提升医生出诊率，创新模式降低患者爽约率。首先应建立严格的停诊制度和审批流程，通过建立参与预约挂号医生的管理规范，将门诊医生失约列入缺陷管理，作为科室和个人年终考核指标，可以极大地提高医生的出诊率[10]。(2) 信息公开，保证预约挂号公平及公正。对于预约和窗口两种挂号方式的优先性问题，根本解决之道在于挂号信息公开，挂号模式公平以及给患者提供特殊情况下的救济措施。

参考文献：

[1] 杨红，黄于梅. 电话预约挂号闭环式服务模式实践与效果[J]. 现代医院，2011，11(1)：111-112.

[2] 洪俊，陈庆瑜，吴媛萍，等. 预约挂号需要完善配套服务措施[J]. 现代医院，2011，11(2)：99-100.

[3] 周琳，李刚荣，李晴辉. 预约挂号系统的设计与实现[J]. 重庆医学，2009，38(11)：1413-1415.

[4] 戴黎阳，曾凡，康运生. 医院网上挂号预约系统的设计及相关问题探讨[J]. 重庆医学，2009，38(21)：2665-2666.

[5] 李翔，唐慧. 多方式实时付费预约挂号平台的设计与实施[J]. 中国医院管理，2011，31(5)：70-71.

[6] 张秋霞，汪洪明，郑彩娟. 实行门诊预约挂号分时段就诊服务的体会[J]. 医院管理论坛，2011，5(28)：32-33.

[7] 赵存现，徐兴勇. 就诊看病实名制的探讨及应对措施[J]. 重庆医学，2009，38(4)：492-493.

[8] 穆云庆，李刚荣，赵存现. 基于“城市一卡通”的门诊就医流程设计[J]. 重庆医学，2009，38(13)：1568-1569.

[9] 钟红玲，刘春生. 大型综合性医院建立“一站式”门诊服务模式探索与实施[J]. 重庆医学，2010，39(10)：1305-1306.

[10] 姜贤飞，谢娟. 门诊预约挂号难点与对策分析[J]. 中国循证医学杂志，2011，11(2)：234-236.

(收稿日期：2011-09-07 修回日期：2011-09-20)

·经验交流·

医院与医保联网存在的安全风险和解决方案

曾 凡，于鸿飞，黄 昊

(第三军医大学大坪医院野战外科研究所信息科，重庆 400042)

摘 要：目的 探讨医院与医保联网存在的安全风险与解决方案。**方法** 通过分析医院与医保联网的安全风险，提出医院与医保联网的安全数据交换方案。**结果** 建立由医院方独立管理和控制的数据安全交换网关，可实现医院医保联网的信息安全目标。**结论** 隔离网闸和安全网关技术是确保医院医保联网信息安全的有效解决方案。

关键词：医院信息系统；计算机安全；保险，健康

doi：10.3969/j.issn.1671-8348.2011.35.011 **文献标识码：**B **文章编号：**1671-8348(2011)35-3562-03

随着中国医疗保险制度的推进，医疗保险范围不断扩大，有越来越多的人参加医疗保险，也有越来越多的医院成为医保定点医院[1]。医院在对医保患者提供医疗服务的时候，需要与该地区的社会保障部门进行信息交流，主要是为享受社会医疗保障的人员提供个人参保情况、费用等一系列数据，大部分医院都与当地医保信息中心进行了网络互联[2]。由于医院信息系统的性质和特殊要求，如何在进行网络互联为医保患者提供医疗服务的同时，可靠地保障医院内部的信息安全[3]，是医院信息化建设中需要解决的重要问题。

1 医院网络与医保网络之间的网络现状及安全风险分析

1.1 医保网络情况 中国劳动与社会保障部门对医疗保险采用的是集中支付的运行模式，医保信息网络必须与医院、政府、

社区、药店、银行、财政等多个相关单位进行连接，以便获取必要的参保人员信息，并进行对应的支付服务。因此，医保网覆盖面广，网络结构非常复杂，管理难度很大。

1.2　医院网络与医保网络的连接情况　医院网络通过与医保网络的连接来为医保患者提供医疗费用的核销等保障服务。医保信息中心与医院、药店、社区等各个单位之间的数据交换采用类似银行的前置机加防火墙模式，其特点是：在医保网络与医院网络之间，放置一台前置机和防火墙，双方的数据交换都通过防火墙与前置机相连来完成，互相不进入对方的区域[4]。

1.3　医院网络与医保网络之间的数据交换方式　医院网络与医保网络之间的数据交换是采用数据交换接口来实现。医保接口是连接医疗保险与诸多定点医疗机构之间的桥梁，完成医保中心与医疗机构之间的信息传送，主要包括了卡读写、帐户圈存、数据传输、医保算法等多方面的内容[5-7]。该接口部署在医院信息系统网络的终端上，例如：挂号室的终端、住院部的终端、收费处的终端以及医院信息系统（HIS）的服务器上[8-10]。

1.4　存在的安全风险分析　从目前实际情况分析，医院网络与医保网络互联中存在的主要安全风险包括“三个不可控”。即网络安全环境不可控、网络范围不可控、核心服务器主机安全不可控。（1）网络安全环境不可控。医保信息网络环境异常复杂，从业务工作需要，除内部联网外，还必须和医院、银行、社区街道、药店等单位互联，其中一些受地理条件限制的社区街道只能通过互联网与医保中心连接。实际上，医院网络通过医保网络与互联网间接相连。因此，来自网络环境的威胁是必然存在的。（2）网络范围不可控。医保信息中心通过城域网的“专线”与医院网络互联，对于这个“专线”的概念存在误区，由于数字网络的特点，这种“专线”仅仅是医院网络到城域网机房之间的“专线”，并不是想象中的医院网络与医保网络的“专线”，而是医院网络和医保中心之间通过在城域网交换机上设置虚拟局域网（VLAN）来实现逻辑上的“专线”[10]。目前最常见的是采用多协议标签交换（MPLS）技术实现虚拟专线[11]，这种专线可以通过人为设置进行改变，甚至允许任何节点访问，因此，医院通过不可控的各地城域网连接医保网络，就需要各地城域网的网络管理严谨、可靠，这些存在巨大的不确定性。（3）核心服务器主机安全不可控。放置在医院网络与医保网络之间的前置机，在实际工作中只能由医保中心方面进行管理和配置，医院方面对该服务器没有控制权。前置服务器安装了 Windows 操作系统、医保应用软件等，存在大量系统漏洞，且由于网络原因，其补丁更新常常不及时。该服务器前端虽然设有防火墙，但防火墙采用在网络层上的逻辑隔离机制，即主要通过软件策略来实现，由于在网络层是相通的，所以很难终结有经验的黑客，无法防止内部信息泄漏和外部病毒、黑客程序的渗入，安全性无法保证[12]。

2　医院网络与医保网络安全数据交换方案设计

2.1　安全风险解决对策　在医院网络与医保网络互联中，主要的安全风险在于：医院网络与医保网络之间没有医院方面可控的安全网关，也就因此失去了对网络安全包括信息安全交换方面的主导权。因此，解决医院网络与医保网络之间安全数据交换的对策就是在医院网络与医保网络之间，建立由医院方独立管理和控制的数据安全交换网关，实现以下安全目标：（1）能够有效断开互联网与医院网络间的网络连接；（2）能够限制访问医院网络的外网主机数量，只允许医保前置机访问医院网络；（3）具备很强的自身抗攻击能力，防止被黑客攻击保证对网络传输的控制权；（4）能够有效阻断病毒、木马向医院网络终端的传播或远程控制医院终端；（5）能够有效防止医院网络终端通过医保网络线路向外泄露 HIS 数据；（6）采用有效认证与访问控制机制，保证只有授权的医院终端能够访问医保前置机。

2.2　安全网关硬件平台的选型　要实现医院网络与医保网络传输通道的有效控制，首先是采用可靠的硬件平台，该平台应具备极强的抗攻击能力，并且保障医院网络与医保网络之间间接连接的 Internet 线路实现完全网络断开。本方案设计采用安全隔离与信息交换系统（即隔离网闸）作为基础硬件设备实现对医保网络连接信道的访问控制和网络隔离。安全隔离与信息交换系统内部连接采用硬件开关进行连接，在没有数据交换时，所有开关均断开，保证内、外网物理断开。有数据交换时，例如从左边交换到右边，也是先接通左边一侧的开关，右边的开关仍旧断开，等数据完全进入系统内部隔离卡中后，再断开左边开关，接通右边开关，将数据传输到右边。因此，即使在有数据交换时，内外网也始终处于网络断开状态。由于硬件的处理动作很难像软件一样被黑客控制，因此，这种以硬件为基础的安全网关具备很高的抗攻击性[13]。

网闸的工作原理是：信息通过网闸传递需经过多个安全模块的检查，以验证被交换信息的合法性。当访问请求到达内外网主机模块时，首先由网闸实现传输控制协议（TCP）连接的终结，确保 TCP/IP 协议不会直接或通过代理方式穿透网闸；然后，内外网主机模块会依据安全策略对访问请求进行预处理，判断是否符合访问控制策略，并依据服务访问接口协议（RFC）或定制策略对数据包进行应用层协议检查和内容过滤，检验其有效载荷的合法性和安全性。一旦数据包通过了安全检查，内外网主机模块会对数据包进行格式化，将每个合法数据包的传输信息和传输数据分别转换成专有格式数据，存放在缓冲区等待被隔离交换模块处理。这种“静态”的数据形态不可执行，不依赖于任何通用协议，只能被网闸的内部处理机制识别及处理，因此可避免遭受利用各种已知或未知网络层漏洞的威胁[14]。见图 1。

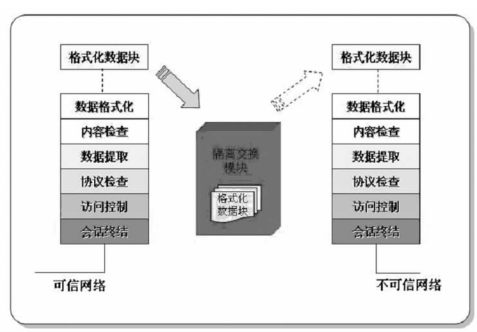

图 1　网闸的工作原理模块图

2.3　身份认证与访问控制系统设计　身份认证和访问控制系统是信息安全的基础组件，医院网络与医保网络的互联应具备完善的认证与访问控制功能。包括：（1）源、目的 IP 地址访问控制；（2）源、目的 TCP 端口范围访问控制；（3）TCP、UDP、ICMP 通讯协议类型控制；（4）访问时间控制；（5）访问 IP&MAC 地址绑定控制；（6）访问者用户名/口令或 USB Key 数字证书认证；（7）单/双向通讯（访问方向）控制。采用安全隔离与信息交换系统结合安全网关可以实现上述访问控制功能。医院网络端访问医保前置机的终端主要集中在挂号、收费、住院等窗口，且主要访问方向为医院端到前置机端，医保前置机主动访问医院网络的情况极少。因此，管理员通过上述认证和访问控制规则，能够严格控制医院网络与医保网络间的访问活动，禁

止除医保前置机外的任何外网节点访问医院内网，禁止任何外网主机直接访问医院 HIS 等核心服务器，同时，也禁止医院网络主机向除医保前置机外的任何其他 IP 地址发起访问，限制医院网络能够访问医保前置机的终端数量。

2.4 木马与病毒防御系统设计 本方案设计的一个重要目标是能够有效防止木马、病毒等对医院网络的攻击。主要采用基于应用程序白名单认证机制，能够有效解决病毒、木马对系统产生的安全威胁。与传统的防病毒、主机 IPS 主动防御系统比较，除能够防御已知病毒、木马攻击以外，还能有效防御未知病毒、木马的攻击。白名单的缺点是无法满足任意访问的互联网环境，但在本项目中没有任何障碍，因为访问的目标明确，访问主机是医保前置机，访问的协议是数据库 SQL 或医保封装的访问接口，访问的程序是 HIS 客户端或医保提供的客户端程序。

3 系统部署方式及应用

本项目的网络部署方式为客户端与网关部署相结合，在需要访问医保网络的客户端安装主机安全防御套件，该软件保护主机在使用医院 HIS 客户端或医保客户端访问医保前置机时，不受任何病毒、木马的感染和破坏，同时，该套件与安全网关联动，由管理员通过安全网关配置客户端防御套件的安全属性，强制进行身份认证、IP、端口、访问方向等一系列安全控制，构成动态的防御体系[15]。在医保网络前置服务器与医院网络之间部署安全隔离与信息交换系统（隔离网闸）和安全网关，实现医院网与医保网间的网络物理隔离断开与数据的摆渡交换。

4 结 语

由于医疗保险业务的需要，使得医院内部计算机网络与其他网络出现了直接或间接的互联，这给医院信息安全造成了巨大的威胁，采用隔离网闸技术和安全网关技术，进行网络安全控制，是一种有效的解决方案，它既实现了医院内部计算机网络与其他网络的物理隔离，保证了医院内部计算机网络安全，又不影响医疗保险业务的正常进行。

参考文献：

[1] 代剑，周睿，徐永刚，等. 医院信息系统与医保联网的问题与对策[J]. 重庆医学，2007，36(23)：2379-2380.
[2] 刘剑锋，李刚荣. 定点医疗机构医保信息化建设的问题与对策[J]. 重庆医学，2008，37(21)：2406-2407.
[3] 巩蕾，王伟伟. 关于 HIS 与医保系统之间接口的认识[J]. 医疗装备，2010，23(1)：45-46.
[4] 朱玉芝，石磊. 谈医院信息系统与医保系统联网的安全体系架构[J]. 中国医药导报，2008，5(29)：74-75.
[5] 代剑，郭斌，范亚川，等. “军卫一号”与新型城乡合作医疗接口的实现[J]. 重庆医学，2009，38(21)：2660-2661.
[6] 沈宁乔. HIS 系统与多套异种医保系统的连接[J]. 医学信息，2010，2(9)：3059-3060.
[7] 马继锋，张怀亮. 医保/新农合系统和 HIS 系统接口的设计和实现[J]. 医学信息，2010，23(11)：3941-3943.
[8] 张暄，唐晓东. HIS 与医保系统接口程序设计方案及实现[J]. 实用医药杂志，2009，26(1)：69-71.
[9] 叶俊，刘松林，李立. 出入院管理系统与医保、农保接口解决方案及其实现[J]. 医学信息，2009，22(8)：1409-1410.
[10] 曾幸辉. 用 VPN 解决方案实现社保局与医院联网的探讨[J]. 教育技术导刊，2008，7(9)：113-114.
[11] 董元和. 基于 MPLS VPN 的安全一卡通网络的研究与设计[J]. 湖北师范学院学报：自然科学版，2011，31(1)：36-39.
[12] 刘晓辉，李利军. 交换机·路由器·防火墙[M]. 北京：电子工业出版社，2007.
[13] 陈征，刘刚杰. 网闸在社保网络安全防护中的应用研究[J]. 网络安全技术与应用，2008(8)：70-72.
[14] 潘诚. 隔离网闸在民航空管信息安全中的应用[J]. 电脑知识与技术，2010，29(6)：8373-8375.
[15] 林达峻，任忠敏，干峰，等. 隔离网闸在医疗行业中的应用[J]. 医学信息，2010，23(9)：3284-3286.

（收稿日期：2011-09-06 修回日期：2011-09-20）

·经验交流·

机房智能系统的设计与实现*

陈利佳，李刚荣△，汪 鹏，周 琳
（第三军医大学西南医院信息科，重庆 400038）

摘 要：目的 利用智能机房系统（ICS）保障计算机数据网络中心机房的设备正常运行。**方法** 使用工业级计算机网络和工业控制系统的仪表、传感器、执行器、控制器等设备，构成稳定可靠的自动化系统。**结果** ICS 对机房运行环境、电力状况、安全保障、消防灭火报警等能自动监视控制处理，保障了计算机数据网络中心机房的设备正常运行。**结论** ICS 是一个综合性很强的系统工程，利用多学科综合技术在现有的技术装备基础上，进行技术开发和改造，用很少的投入实现其中的部分重要功能，达到节省人力物力、提高机房安全保障和管理水平。

关键词：人工智能；自动化；软件设计；智能机房系统
doi：10.3969/j.issn.1671-8348.2011.35.012 **文献标识码：**B **文章编号：**1671-8348(2011)35-3564-03

智能机房系统（intelligent computer-room system，ICS）是为了保障机房的设备正常运行，使用工业级计算机网络和工业控制系统的仪表、传感器、执行器、控制器等设备，构成稳定可靠的智能控制系统（图 1），从而完成对机房网络、环境、电力等状况自动监视、控制和处理。ICS 的应用，在国外已经流行多年。随着中国计算机应用的普及和发展，ICS 也逐步在许多行

* **基金项目：**重庆市科技攻关计划资助项目（CSTC，2007AC2048）。 △ **通讯作者，**Tel：13883404928；E-mail：13883404928@163.com。