网络隔离与交换技术在 HIS 中的应用

摘要：

医院信息系统（HIS，Hospital Information System）是现代医院中最基本的管理信息系统，HIS 是计算机技术、网络通信技术和现代管理科学在医院信息管理中的应用，是计算机技术对医院管理、临床医学、医院信息管理长期影响、渗透以及相互结合的产物，它利用计算机网络来传递、保存信息，使信息在大范围内实现实时共享。**医院是国内知名医院之一，素有南**、北**之名。本文简单的描述了该医院的内外网的物理隔离模式，同时讲述了为了实现内外网之间的数据安全交换，满足 2 个物理网络间的信息交换及数据同步不断增大的需求而采取的网络隔离和安全交换技术。同时，本文在介绍了网络隔离与安全交换技术的基础上，研究了网络隔离与安全交换系统在 HIS 中的应用，设计并实现了基于网络隔离与安全交换技术的检验结果查询系统。最后本文给出指出了网络隔离与安全交换技术应用效果。

全文：

我作为**医院信息中心的负责人，主要负责医院信息系统（HIS）的系统设计与分析、网络运维、网络安全保障等工作。目前，考虑安全和保密的要求，**医院的 HIS 几乎全部运行于医院内部网络中，与国际互联网和其他公共信息网络没有连接。医院的信息只能在医院内部得到利用，患者还不能通过互联网和短信等公共信息平台合法地获取相关信息，如为了得到检验结果，有时患者要往返我院多次，化验单丢失现象也时有发生。换言之，信息技术并未有效改善和提升患者的就医效率。

医院 HIS 的发展面临着既要保证安全又要进行信息交换的难题。本文在介绍了网络隔离与安全交换技术的基础上，研究了网络隔离与安全交换系统在 HIS 中的应用，设计并实现了基于网络隔离与安全交换技术的检验结果查询系统，解决了内网中的检验结果数据通过外网安全发布的问题，有效地改善和提升患者的就医体验。同时对网络隔离与安全交换技术在 HIS 上的深层应用进行了展望。

1. 网络设计与分析

经过多方研究与调研和依据我们在行业这么多年的经验，我们选择了网络隔离与安全交换技术。

网络隔离与安全交换系统的基本理念是在切断内、外部网络间直接连接的同时，结合访问控制、身份鉴别等安全机制，实现不同安全等级网络间安全的数据交换。我院采用该技术理由如下：

（1）该技术通过在切断直接连接的网络间建立对用户透明的逻辑“连接”，把客户/服务器连接划分为 2 个完全独立的安全连接，并通过特定的协议实现 2 个连接之间的数据安全交换。

（2）可以根据 RFC 规范对协议进行细粒度检查。

（3）可以实施多种安全策略和防护措施，包括内容过滤、认证与授权、访问控制等附加安全功能。

通过允许原始应用数据进入的技术手段保证内部网络和外部网络的安全隔离，主要解决不同安全等级网络间的数据交换问题，防止内网的资源被隔离对象以外的人员访问，并保证交换数据的完整性、实时性。结合网络隔离系统上的网络应用，根据不同的数据服务，对内外网之间通信的数据内容进行过滤，防止未经允许的内网数据发生泄露。网络隔离与安全交换是一种非常安全的网络安全技术，第一，不采用 TCP/IP 协议或其他通用网络协议传输数据，而是通过专用协议传输特定数据。因此，网络隔离与安全交换技术有效地阻止了基于通用网络协议对内部网络的攻击。第二，内外网之间没有直接或间接的网络连接。因为互联网是基于 TCP/IP 协议来实现的，而大多数攻击都可归纳为对基于 TCP/IP 协议的数据的攻击。因此，断开 TCP/IP 的连接，就可以消除目前 TCP/IP 网络存在的攻击。第三，网络隔离与安全交换技术不依赖操作系统，采用网络隔离与安全交换技术的设备运行在专用操作系统上。不依赖通用操作系统有效地降低了利用操作系统漏洞进行攻击的威胁。

网络隔离与安全交换技术交换的是原始的数据，这些数据只会传送给特定用户，而且在数据传输到用户之前允许对数据内容进行审查，通过这些措施可以达到安全防护的目的。

2. 网络隔离与安全交换系统体系架构设计

网络隔离与安全交换系统由内部网处理单元、外部网处理单元和控制处理单元 3 个逻辑部件组成。如图 1 所示内网单元与内网相连，外网单元与外网相连。控制单元是内网单元与外网单元之间唯一且安全的数据通道，负责在保证内、外网隔离的前提下，对要交换的信息进行安全检查只有符合安全保密策略的信息才能被交换。

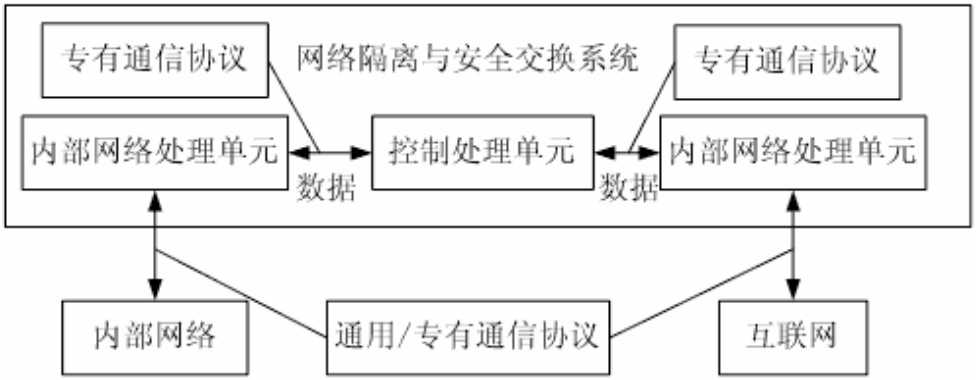

图1 网络隔离与安全交换系统体系结构

内、外网单元应采用安全操作系统或公开源代码且经过安全性增强的操作系统。内、外网单元是由独立的硬件设备组成的，能够独立地完成代理网络请求、日志审计、访问控制与授权等功能的处理机。各网络安全处理单元既相互独立，有效实现内外网的相互隔离,同时又协同工作，完成内外网之间授权数据的可靠、高效传输。彼此独立的网络安全处理系统被封装在一个相对安全的物理环境内，彼此通过安全的通信信道完成数据交换。

3. 网络隔离与安全交换应用方案设计

我院的网络布局为典型的内外网完全物理隔离模式，分为 HIS、LIS、PACS、OA 等内部网络和网站、随访中心、远程挂号等外部网络。在网络建设初期，由于网络可用资源较少，内外网之间基本无数据交换，或单纯通过人工拷贝方式来完成。但随着 HIS 建设初具规模，

医院信息化的不断发展，2 个物理网络间的信息交换及数据同步需求增大，由人工拷贝方式来完成内外网间的数据交换，从效率和可靠性上都是不现实的。采用网络隔离与安全交换技术实现内外网之间的通讯，避免了内网 HIS 成为“信息孤岛”，同时也最大限度地保障了信息交换的安全性。

目前，医院 HIS 积累了大量的信息资源，但这些资源利用率普遍偏低。而且医院的信息只能在医院的内部得到利用，各个兄弟医院之间也很难实现数据共享和交换，患者还不能通过公共信息平台合法获取相关信息。采用网络隔离与安全交换技术有效地解决了以上问题。

应用网络隔离与安全交换技术实现医院内网和外网之间的数据交换，不仅能够实现远程挂写，检验结果查询等方便患者的功能，而且能够实现各兄弟医院 HIS 之间、医院与医保中心之间、医院与卫生部门之间的信息安全共享和交换。同时有利于医疗数据深层次的数据挖掘、分析和利用，对决策和管理产生重大的影响。

4. 项目中的关键技术

应用网络隔离与安全交换技术的原理，设计并实现了 HIS 中 LIS 检验结果的短信查询系统，使患者通过短信查询自己的检验结果，作为网络隔离与安全交换技术在医院 HIS 中的试点。

检验结果查询系统包含网络隔离器、内网主机、外网主机和短信收发设备 4 部分组成。网络隔离器与两端主机采用串口 RS232 交叉线连接，内网主机能够访问 HIS 数据库中的检验结果记录表;外网主机负责对接收到的短信进行解析，生成数据库查询语句，对查询结果进行短信发送。

网络隔离器技术实现隔离是关键。正常情况下，网络隔离器和外网、内网之间，外网和内网之间是完全断开的。

（1）当内网需要有数据到达外网时，隔离器与内网接口打开，而隔离器与外网接口关闭。

（2）数据以明文形式发送到网络隔离器中，然后隔离器对进行加密。

（3）加密完成后，隔离器与内网接口关闭，而隔离器与外网接口打开。

（4）加密后的数据被发送到外网主机中，由运行在外网中的应用程序进行解密。这样不仅实现了网络隔离，又实现了数据的安全交换。

5.小 结

应用网络隔离与安全交换技术实现医院内网和外网之间的数据交换，实现检验结果查询系统作为试点。该系统在应用层面对要交换的数据类型进行了严格的限制，通过私有协议传输，与采用协议净化控制功能的安全网闸相比，数据安全控制方面更强，而成本却较低，此系统为 HIS 中数据安全交换提供了新的途径。由于查询系统是通过短信方式进行的，患者需要使用其 ID 号+患者姓名+检验申请时间构成查询短信内容来进行查询，这样对于一些年纪较大的患者来说，非常不方便，在今后的项目改进中，我们将考虑采用多种查询方式进行查询。