表 5　测试灵敏度、特异度

	规则（1）		规则（2）		规则（3）	
结　果	高血压	非高血压	肺心病	非肺心病	冠心病	非冠心病
阳性例数	49	0	5	0	8	0
阴性例数	0	15	1	49	1	45
灵敏度	100%		83.30%		88.89%	
特异度	100%		100%		100%	

由表 5 的结果可以看出，用以上三条规则对预测样本进行判别，判别结果灵敏度和特异度都相当高，即漏诊率和误诊率都很低，并且挖掘出来的三条规则在临床上也能得到很好解释。

3　讨论

首次将粗糙集应用到心脏超声诊断上，取得了令人满意的效果。借助粗糙集理论运用软件 -Rosetta 对决策表进行属性约简，大大地减少了属性约简过程的计算量和难度，容易被一般的临床医生掌握。它把心脏超声实测指标与知识挖掘有机的结合起来，避开了求取隶属度等主观因素，引进了严格的数学理论，提高了心脏超声诊断的思维逻辑的严密性，为临床诊断展示了潜在的前景。

[参考文献]

[1]刘洪艳. 基于粗糙集的数据挖掘[J].甘肃教育学院学报(自然科学版), 2002,16(3):18-20.

[2]秦中广. 粗糙集在中医类风湿证候诊断中的应用[J].中国生物医学工程学报, 2001,20(4):359-363.

[3]于 洪.基于粗糙集理论的数据挖掘的应用[J].计算机与现代化, 2001,4:45-53.

[4]王向阳,崔 林,褚玉林. 基于粗糙集理论的医院院内感染数据挖掘[J].洛阳工学院学报, 2002,23(2):59-62.

编辑 / 任鸿兰

健康体检计算机管理系统安全解决方案

包国峰[1]，石 冰[2]

（1. 山东省立医院信息网络中心，山东 济南 250021；　2. 山东大学计算机科学与技术学院，山东 济南 250061）

摘要：本文在健康查体计算机管理系统的基础上，提出了基于体检系统的安全解决方案。通过多因子 CHAP 协议和个人智能密钥的应用，实现了身份验证和数字签名。通过多因子认证安全服务器，建立综合安全服务平台，保证了整个业务系统的安全性。

关键词：健康体检；安全方案；　数字签名

1　概述

健康体检计算机管理系统是针对目前广泛开展的健康查体业务，为提高查体效率、规范查体医务、方便查体人群、为医教研提供可靠详实的查体资料而设计的计算机网络化处理系统[1]。它取代了大量的检查单据，优化了体检流程，提高了查体效率，正在为越来越多的专业体检机构所使用。如何保证系统不被非法用户进入和使用，保证电子体检报告的真实准确性，保证体检数据不被非法或意外修改，也就是体检系统的安全问题，成为当前急需解决的关键问题。

2　系统的安全需求

体检计算机管理系统中包含大量重要的体检数据，其准确性直接关系到体检部门的业务声誉和参检人员的健康，因此在整个系统的建设中必须从系统、网络、应用和数据等各个层面建立严密的安全体制，做到对系统和数据的完善保护。

2.1　身份验证

目前应用的体检系统主要采用用户名加密码的方式，因此可以很简单的猜出别人的密码，以他人的身份进入系统，造成系统数据混乱，存在严重的安全隐患。采用更为安全的身份验证机制，是体检系统的普遍需求。

2.2　电子体检报告的安全保护

电子体检报告是体检信息系统发展完全化的一个结果，是以体检人员为中心的信息集成与相关信息服务。它不仅包括参

收稿日期：2004-08-18

检人全部的体检信息(数字、文字、图形、图像),而且还包括丰富的医学知识与联机服务。因此,必须对电子体检报告进行严格的安全保护,建立可行的电子体检报告的验证机制。

2.3 权限控制

体检系统中的权限控制关系到对各项业务模块及各类数据的访问权限,对于整个系统的安全具有重要的意义。目前的体检系统一般还没有权限认证及访问控制机制,一切的控制建立在用户名加密码的认证机制之上,对系统管理员没有任何访问权限控制,造成对数据及功能模块的随意访问与操作,因此存在严重的安全隐患。

2.4 加密存储

目前一般的体检系统无法完成电子体检报告及其他重要数据的加密存储和访问控制。首先没有权限确认,电子文档也没有相应的访问控制,因此导致系统用户可以任意访问所有的体检报告。其次由于电子体检报告和数据没有加密存储,系统维护人员或相关人员可以通过访问数据库获得电子体检报告信息,给体检工作的日常管理带来了安全隐患。

2.5 数据的安全传输

目前,体检系统主要依托医院内部局域网运行,由于系统所采用的 B/S,C/S 方式本身就具有的开放性等特点,所以在体检管理系统的规划与设计过程中,必须考虑敏感数据在网络上传输时的加密问题,防止数据的泄露。

3 安全方案的设计原则

3.1 安全性

必须针对体检管理系统的特殊需求,提供有效的安全保障,保证网络系统、服务器系统、存储系统、操作系统、数据库系统和应用系统的安全,提供完整的基于 Intranet 和 Internet 的安全保密机制。

3.2 实用性

以用户需求为基准, 实现与现有体检系统的无缝衔接,保证体检业务系统的正常运行。

3.3 先进性

必须保证技术的先进性, 符合未来发展的趋势与需求,建立高强度的统一安全平台。

3.4 高集成性

强调安全系统的标准化,系统应能保证与现行体检业务系统实现有效的衔接,实现信息的交换、共享和集成。

3.5 可扩展性

安全系统的建设不仅要满足当前的需求,还应具备良好的可扩展性,随着业务功能和用户数量的增加与变化,提供方便快捷的实施与升级方案。

3.6 稳定性和可恢复性

保证系统的稳定性。确保在出现问题时能及时、准确地恢复系统。

3.7 可管理性

安全系统的使用及管理应以简便、易于操作、方便实用为准则,保证安全系统具有高可管理性,降低系统管理和维护成本。

4 系统安全方案的设计

体检管理系统安全解决方案是对系统的完善与优化,通过构建统一的安全认证平台, 提供了对现有系统的接口支持,容易部署与实施。通过为用户提供个人智能密码钥匙,实现网上的身份认证、数据加密和关键数据的存储。通过提供多因子认证安全服务器,建立综合安全服务平台,保证了整个业务系统的安全。

4.1 方案拓扑图

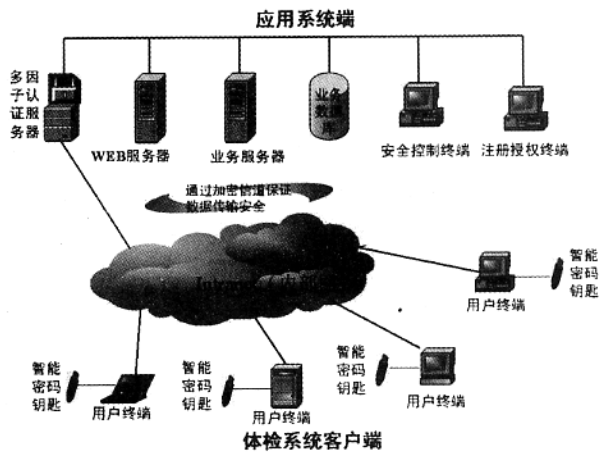

图 1 方案拓扑图

图 1 中的业务服务器和业务数据库代表目前运行的体检管理系统,通过建立在智能密码钥匙和认证服务器之间的多因子 CHAP 协议,根据验证方与被验证方之间的三次信息交互(握手)来验证访问者身份,从软件到硬件保证了用户身份的真实性和唯一性。在用户身份通过认证后,对体检业务流程中沿网络传输的数据提供安全保障,并实现对电子体检报告的加密存储与访问控制,从而实现对体检系统中从登录到存取的各业务环节的安全保障。

4.2 多因子身份认证

解决身份认证安全问题。身份认证主要是通过特定的技术来鉴别当事人身份的安全性保障措施。多因子安全身份认证系统在用户进行登录时,首先要通过口令或指纹的方式成功的开启个人智能密钥之后, 才可以进入系统进行身份认证,这提供了比普通口令、密码认证身份高得多的安全级别,即使在密钥丢失或被盗的情况下,没有正确的密码或指纹输入是无法使用系统的;在成功开启密钥后,密钥和认证服务器之间通过多次交互对用户的身份进行鉴别,快速安全地进行用户身份的合法性认证。

4.3　数字签名

建立电子体检报告的安全验证机制。电子签章系统既可以实现数字化电子印章,也可以实现数字化手写签名,直观、形象、简便、安全的实现对电子体检报告的保护。向密钥中灌入电子印章数据是经由多因子认证安全服务平台进行签名的,确保印章放于密钥中不能伪造;签名运算在密钥内进行,绝对保证签名私钥保密。密钥采用 PKI 技术,以 RSA 算法实现数字签名,符合未来电子签名法的规范。由于生成签名的因子只存储于用户的密钥中,具有更高的安全系数。

4.4　访问权限控制

在安全系统的搭建过程中, 建立起角色的权限分配机制,角色的权限与个人密钥关联起来,所有授权工作是在两个具有管理权限的人同时在场才能完成的工作,防止系统管理员独自修改权限而浏览份外的资料,确保合法的、具有权限的用户才能获得数据库中存储的相关资料。

4.5　数据加密存储

解决体检数据的加密存储,防止恶意察看。数据库的加密密码由认证服务器提供,数据保存到数据库表中,系统对部分关键数据进行加密处理,密码与数据库表的字段、记录号关联,使得每个表中每个记录、每个字段都有不同的密码,提高加密强度。只有具有访问权限的用户持有个人密钥在身份认证之后,才有可能通过加密传输通道从服务器端获取数据。没有访问权限的用户则无法访问数据库,即使是系统管理员,也只能完成他份内的管理工作,而对关键的数据库信息无能为力。该安全方案中设计的角色、权限不是传统意义上的软件管理方式,而是结合了智能密钥硬件,把角色、权限信息保存到了硬件中,任何个人都无法修改,确保了数据的安全性。

4.6　数据安全交换

解决数据在传输过程的加密问题,保证只有有权限的人才能够获得相关数据。①智能密钥的持有者,通过认证服务器的身份认证。②建立智能密钥与认证服务器之间的加密通道。③认证智能密钥持有者的角色、权限。④通过加密通道进行加密数据的交换。如果是发送到服务器端的数据,则通过认证服务器提供的接口,先对客户传送过来的数据用通道密码解密,然后根据数据库表、字段、记录号等信息产生数据加密密码,加密后保存到数据库中。如果是客户端请求数据,则智能密钥持有者在身份、角色、权限认证无误之后,从数据库读出所需的数据记录,经由认证服务器进行数据解密,然后再对数据使用加密通道密码加密,发送到客户端。通过客户端智能密钥对加密通道传送过来的数据解密后,展示到客户端界面。

5　结论

该方案从系统、网络、应用和数据等各个层面建立了严密的安全体制,做到了对体检系统和数据的完善保护。为全面实现数字化查体医务和电子体检报告奠定了安全基础。

[参考文献]

[1]包国峰 . 一卡通电子查体医务系统的设计[J]. 医学信息,2003,16,(9):477.

编辑 / 晁慰亮

我院信息服务形式的拓展及效果分析

李顺飞,罗　娟,吕　强

(解放军第 150 中心医院信息科,河南 洛阳　471031)

摘要:随着医疗市场竞争形势的日趋严峻,医院的医疗质量显得尤为关键。医院信息系统 HIS(Hospital Information System)的开发与应用为处于高竞争压力下的医院现代化管理奠定了基础,同时也对医院信息服务提出了新的机遇和挑战。本文论述了我院基于医院信息系统拓展信息服务形式的实例。

关键词:信息服务;　医院信息资源;　网络信息资源

随着医疗保障体制改革的深入,人们对医疗服务质量提出了更深层次的要求。医院信息系统的逐步完善,为医院现代化管理提供了科学详实的信息资源。目前,国内医院对信息资源的利用严重滞后于医院信息系统的建设水平,其信息服务形式单一、信息服务质量跟不上,严重地影响信息资源的利用。只有充分挖掘管理者的决策需求、业务人员的知识需求,对网络信息资源进行整合加工,提供更为科学实用的信息服务模式,才能促进网络信息资源的高效利用。我院在

收稿日期:2004-05-18