医疗行业数据安全探析

袁 琛

（天津市人民医院 天津 300130）

〔摘要〕 从分析医疗行业数据安全角度出发，指出数据安全存在的隐患和数据泄露原因，结合医疗机构特点着重在技术防护方面详细阐述数据安全防护策略，包括身份鉴别、自主访问控制等方面。

〔关键词〕 医疗行业；数据泄露；数据安全；技术防护

〔中图分类号〕R－056 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2016.02.009

Analysis of Data Security in the Medical Industry *YUAN Chen, Tianjin People's Hospital, Tianjin 300130, China*

〔**Abstract**〕 By analyzing data security in the medical industry, the paper points out hazards existing in data security and reasons for data leakage. In combination with characteristics of medical institutions, it elaborates strategies for protecting data security with an emphasis on technical protection, including identity authentication, discretionary access control, etc.

〔**Keywords**〕 The medical industry; Data leakage; Data security; Technical protection

1 引言

随着我国医疗信息化步伐的加快，医院信息化程度不断提高，几乎与诊疗相关的数据都已电子文档化，而与之伴随的医院数据泄密风险也因此被进一步放大[1]。医疗行业的数据安全面临着非常严峻的考验，这些数据直接关系着医疗机构的发展与患者的隐私。医疗信息安全问题，具体来说是由于管理和外部原因造成的医疗信息泄露、篡改、遗失等问题。医疗数据安全面对的威胁主要来自两方面：一种是黑客攻击导致数据丢失或系统崩溃；另一种是由人员造成的数据泄露。由于医疗数据的特殊性，在保障完整性的同时，需要着重从访问者的身份鉴别、访问控制、保密性、密码支持等方面做好防护，避免非法访问和数据泄露。

〔修回日期〕 2015－10－22

〔作者简介〕 袁琛，工程师，发表论文2 篇。

2 当前医疗行业数据安全形势

2.1 国际

据国际医疗安防与安全协会统计，医疗犯罪数量近年来上升迅速[2]。根据波尼蒙研究所的调查，2014 年美国有 40% 的医疗机构遭受了恶意软件的侵扰，试图盗窃其中的数据，而在 2010 年，这一比例为 20%。2014 年美国 10 家医院中有 9 家曾遭数据泄露或者网络遭入侵。2014 年 3 月 30 日，来自东欧的黑客侵入了犹他州卫生署技术部门的服务器，窃取了约 78 万医疗补助患者和儿童健康保险计划的相关个人数据，有 78 万人受到影响。黑客能够访问这些信息的原因是设置的密码较弱。2014 年 2 月位于加利福尼亚州的圣若瑟医院发现的一个可能的安全漏洞惊动了全国约 31 800 名患者。据查该系统的安全设置是不正确的，可能会发生潜在的数据入侵，造成患者的姓名和医疗数据泄露。

2.2 国内

根据《2014 中国网站安全报告》统计，2014 年 12 月公布的 27 个影响较大的漏洞中，7 个为医疗卫生行业漏洞，每个漏洞都会导致超过百万用户数据泄露[3]。近期又有一波重大网站漏洞被披露，其中很多漏洞集中在一些省市的疾控中心和卫生系统，导致数千万用户的医疗数据可能被泄露。山东省疾控中心某内部系统泄露近 190 万病人信息。导致可以查看近 190 万病人的隐私资料，包含身份证号、姓名、性别、生日、电话、职业、户籍、地址、工作单位、患病情况等敏感信息，以及近 140 万随访信息，其中含敏感资料。泰州市疾控中心某系统泄露全市 68% 的居民（345 万）敏感信息，包含：姓名、性别、年龄、身份证号、家庭关系、地址、电话、患病情况等信息。徐州市疾控中心某漏洞可能泄露全市 80% 居民（763 万）敏感信息，包含姓名、性别、年龄、身份证号、家庭关系、地址、电话、患病情况。

3 医疗行业数据安全分析

3.1 数据安全存在的隐患

数据安全隐患存在于医疗机构信息化流程中的各个环节，无论是结构化或者是非结构化数据的安全防护，均存在一定程度的问题，如技术漏洞、物理故障、恶意攻击等[4]。

3.1.1 *数据交互存在隐患* 相对独立的医疗信息系统制约着医疗数据的交互与上下流动，因此近年来消除这种信息孤岛是医疗信息化建设的重中之重，原有医院内外网物理隔离的架构将面临颠覆性的改变[5]。纵向来看，一方面政策推动医疗机构上传数据，方便主管部门监管医院运营；另一方面区域平台、医联体也需要借助网络实现医疗资源下沉，上至卫计委，下至县医院、村卫生院都分布着信息终端，每个终端都可能成为数据泄露的出口。横向来看，医保系统一方面与医院系统对接，另一方面还要与各级主管部门以及定点药店对接，在数据与业务共享的前提下为参保人提供服务。当然，这一横向的网络上还包括银行、运营商等辅助机构，因此安全威胁的来源也更加广泛，远远不局限于医疗机构内部。除了纵横交错的外在交互，医疗机构自有的公共服务平台也存在安全隐患。比如医院官网，几乎所有三级以上医疗机构都有网站，任何人都可能通过网站对医院服务器发起进攻。

3.1.2 *移动终端存在隐患* 移动通信技术、互联网技术和健康服务正逐步走向融合，将健康服务从计算机平台延伸至手机、平板计算机和任何可移动终端上，实现医患沟通的飞跃[6]。同时无论是 3G、4G 还是 Wifi，都让非法用户可以更方便地入侵医院数据。手机被植入木马后，通过 Wifi、3G、4G 网络就能接入核心业务。Android 系统缺乏合法验证机制，缺乏有效的防护手段，一旦医生使用 Android 系统时从不安全的移动应用商店中下载 APP 就可能被植入木马，再将木马带入医院系统，进而威胁医院数据安全。

3.1.3 *云应用的隐患* 云技术的出现被称为计算机时代的第 4 次革命[7]。医疗机构也在尝试应用云来提升资源利用率。当用户通过云读取数据时，数据从数据中心机房通过云传到用户终端。医疗云平台可能发生大规模的计算资源系统故障，除此之外云计算安全隐患还包括难以对用户隐私、数据主权、数据迁移与传输、灾备等方面进行有效保护。对所发生的安全隐患还缺乏统一的安全标准[8]。据调查医疗机构云服务安全保障有待完善，医疗机构在构建云应用时一定要注意安全保护工作。

3.2 医疗机构数据泄露原因

一是恶意攻击。医疗信息系统除了纵横交错的外在交互，几乎所有三级以上医疗机构都有网站。恶意攻击是医院计算机网络所面临的最大威胁[9]。二是用户帐号。一般来说密码过于简单，容易被盗用，而且很多医护人员缺乏安全意识，帐号密码经常借给别人使用，存在重大安全隐患。此外通常这些帐号管理是单因素的，只有密码，没有其他的手段进行识别。三是审核机制。审核机制相对来说大家重视程度并不高，所以很多的用户操作没有记录、监管，出现问题无法追踪，这也是一个数据完

整性方面的漏洞，并且无法自动识别与阻断数据的非法修改。四是访问控制。有些关键的访问资源无法进行权限控制。医院信息系统在数据安全方面并没有细分权限。系统的开发和维护过程缺乏监管，运维的模式也存在很大的问题。

4 医疗行业数据安全防护应对策略

4.1 概述

在大数据应用、云计算、物联网、移动浪潮等技术概念支撑下及各种利益的驱使下，诊疗信息的泄露风险大大增加[10]。要实现医疗行业数据安全防护，必须紧紧围绕数据自身的安全，从身份鉴别、访问控制、数据完整性、数据保密性、密码支持等多方面规范操作，形成严谨工作流程，确保数据安全每个环节都不出问题。数据安全防护体系的发展趋势是：沿着纵和横两个方向推进，真正做到纵向到底，横向到边，所谓纵深防护就是以应用系统为核心，横向防护就是以终端多样化异构和操作系统为核心，构建一个跨平台、跨设备、跨业务的自主可控的数据全生命周期安全防护体系。

4.2 身份鉴别

（1）用户标识：基本标识应在 SSF 实施所要求的动作之前，先对提出该动作要求的用户进行标识；唯一性标识应确保所标识用户在信息系统生存周期内的唯一性，将用户标识与安全审计相关联；标识信息管理应对用户标识信息进行管理、维护，确保其不被非授权地访问、修改或删除。（2）用户鉴别：一般应按相关要求，设计和实现用户鉴别功能。每次用户登录系统时进行鉴别，鉴别信息应是不可见的，在存储和传输时按国家密码主管部门的规定，分级配置具有相应等级的密码保护。

4.3 自主访问控制

（1）按以下要求确定自主访问控制策略：可以有多个自主访问控制安全策略，但它们必须独立命名，且不能相互冲突。常用的自主访问控制策略包括访问控制表、目录表、权能表等。（2）按以下要求设计和实现自主访问控制功能：SSF 应实现采用一条命名的访问控制策略，说明策略的使用和特征，以及该策略的控制范围。（3）按以下要求确定自主访问控制的范围：对于每个确定的自主访问控制，SSF 应覆盖由安全系统所定义的主体、客体及其之间的操作。（4）按以下要求确定自主访问控制的粒度：主体为用户级，客体为文件、数据库表级和/或记录、字段级。（5）无论采用何种访问控制策略所实现的自主访问控制功能，都能够允许命名用户以用户的身份规定并控制对客体的访问，阻止非授权用户对客体的访问。

4.4 用户数据完整性

（1）要在读取的时候检测存储在 SSOIS 控制范围之内的用户数据是否出现完整性错误，在检测到完整性错误时采取必要的恢复措施，同时分级配置具有相应等级密码管理的密码支持，对加密存储的数据进行完整性检验。（2）SSOIS 能检测出被传输的用户数据被篡改、删除、插入等情况发生，在检测到完整性错误时采取必要的恢复措施，同时分级配置具有相应等级密码管理的密码支持，对加密传输的数据进行完整性检验。

4.5 用户数据保密性

（1）对存储在 SSC 内的用户数据：应根据不同保密性要求，进行不同程度的保护，确保除具有访问权限的合法用户外，其余任何用户不能获得该数据，同时应分级配置具有相应等级密码管理的密码支持。（2）对在不同 SSF 之间或不同 SSF 上的用户之间传输的数据：应根据不同保密性要求，进行不同程度的保护，确保数据在传输过程中不被泄漏和窃取，同时分级配置具有相应等级密码管理的密码支持。（3）按以下要求设计和实现客体安全重用功能：由 SSOIS 安全控制范围之内的某个子集的客体资源，在将其释放后再分配给某一用户或代表该用户运行的进程时，应不会泄漏该客体中的原有信息。

4.6 密码支持

一般应根据密码强度与信息系统安全保护等级匹配的原则，按国家密码主管部门的规定，分级配置具有相应等级密码管理的密码支持，设计和实现由密码机制所提供的安全功能。

4.7 虚拟化安全

虚拟化安全对于确保云计算环境的安全至关重要。因为云计算是利用虚拟化技术实现物理资源的动态管理与部署，为多用户提供隔离的计算环境。

4.8 使用漏洞扫描技术

定期扫描操作系统和数据库系统的安全漏洞与错误配置，及时发现系统中的弱点或漏洞，提示管理员进行正确配置，及时分析和评估，尽早采取补救措施，可避免各种损失[11]。

5 结语

在当今信息时代，医院数据安全变成医疗体系结构中不可或缺的基础架构，作用越来越重要，任何的数据泄露都将对医疗行业造成难以估算的损失。只有做好数据安全防护，才能确保整个行业安全、稳定发展。

参考文献

1 王磊，郭旭升，王颖晶. 医院数据泄密对策研究［J］. 医学信息学杂志，2015，36（4）：36－39.

2 国际医疗安防与安全协会（International Association for Healthcare Security and Safety）. 2012 年犯罪和安防趋势调查［EB/OL］.［2015－06－08］. http：//news.hc3i. cn/art/201309/26815. htm.

3 360 互联网安全中心. 2014 年中国网站安全报告［EB/OL］.［2015－06－08］. http：//www. 360. cn/.

4 邓辉，张宝峰，刘晖. 大数据安全的技术应对策略［J］. 中国信息安全，2015，（4）：105－103.

5 胡芳，沈绍武. 医院信息系统体系架构构建研究［J］. 医学信息学杂志，2012，33（11）：16－21.

6 姚志洪. 跨入移动健康时代［J］. 医学信息学杂志，2014，35（5）：2－7

7 张鑫. 王连根. 胡海荣. 云技术在医院信息化管理中的应用［J］. 医学信息学杂志，2014，（5）：38－42.

8 刘蝉祯. 医疗云平台的安全问题［J］. 重庆医学，2014，43（31）：4157－4159.

9 冉建忠，刘秀华. 浅析医院信息网络安全管理［J］. 计算机光盘软件与应用，2013，（4）：102－104.

10 王晓丹. 当前医疗信息化存在的问题及对策研究［J］. 医学信息学杂志，2011，32（1）：44－47.

11 黄奇华. 计算机信息安全技术及防护研究［J］. 计算机光盘软件及应用，2014，（20）：186，188.

（上接 42 页）

入基于 MOM 数据集成及交换平台和 ODS 来解决目前医院数据不一致和无法共享的问题。在医院中引入交换平台和 ODS 后，通过各种标准，保证数据的及时性和一致性，各业务系统可以从 ODS 通过数据平台来获得所需的数据，实现数据的统一管理，极大地方便数据的使用，为医院后续的信息化建设奠定基础。

参考文献

1 潘志强，吴庆斌. 集成数字证书的非接触式医院一卡通平台设计与应用［J］. 医学信息学杂志，2014，35（12）：31－34.

2 樊泽恒. 校园网功能的理性思考及开发应用的对策［J］. 南京航空航天大学学报，2001，（4）：52－56.

3 郭永生. 基于共享数据库的多数据源集成［J］. 微机发展，2004，14（2）：49－51.

4 秦滔，陈汉利. 基于 XML 消息中间件的公文传递模型研究［J］. 电脑与信息技术，2006，14（3）：57－60.

5 段占祺，应桂英，郑建智. 我国医院决策支持系统建设现状与发展策略［J］. 医学信息学杂志，2014，14（3）：17－20.

6 陈传波，张辉. 基于 XML 和消息中间件的异构数据集成技术［J］. 计算机工程与科学，2005，26（9）：67－70.