“互联网 +”对医院信息系统安全的挑战与对策探讨*

孟晓阳 朱卫国 李连磊

（北京协和医院信息管理处 北京 100730） （中国信息安全测评中心 北京 100085）

苏 博 张 楠 李爱巍 马学泉 黄迎萍

（石化盈科信息技术有限责任公司 北京 100007）

〔摘要〕 分析国内外已经公开的几个安全事件案例，了解其经验教训，结合当前医疗信息技术领域存在的普遍问题，从非军事区、虚拟专用网络、无限局域网、专网专线几方面，探讨“互联网 +”时代医院信息系统面临的安全挑战与应对措施。

〔关键词〕 互联网 +；信息安全；安全边界

〔中图分类号〕 R - 056 〔文献标识码〕 A 〔DOI〕 10. 3969/j. issn. 1673 - 6036. 2016. 12. 009

Discussion on the Challenges and the Countermeasures of "Internet Plus" for the Safety of Hospital Information System

MENG Xiao - yang, ZHU Wei - guo, Department of Information Management, Beijing Union Hospital, Beijing 100730, China; LI Lian - lei, China Informantion Technology Security Evaluation Center, Beijing 100085, China; SU Bo, ZHANG Nan, LI Ai - wei, MA Xue - quan, HUANG Ying - ping, Petro - Cyber Information Co., Ltd, Beijing 100007, China

〔**Abstract**〕 On the basis of analyzing several publicized security event cases at home and abroad, and from which learning the experience and lessons, the paper makes a discussion on the safety challenges faced by the hospital information system in the "Internet plus" era and the countermeasures from the aspects of demilitarized zone, VPN, WLAN, private network and line by combining the common problems existing in the medical information technology field.

〔**Keywords**〕 Internet plus; Information security; Security boundary

1 引言

信息系统安全是信息化建设的基石。按照信息技术安全评价标准（Information Technology Security Evaluation Criteria，ITSEC）的定义，信息安全建设通常包含 3 个重要的目标[1]：保密性（Confidentiality），即确保信息在存储、使用、传输过程中不会泄漏给非授权用户或实体；完整性（Integrity），即确保信息在存储、使用、传输过程中不会被非授权用户篡改，同时还要防止授权用户对系统及信息进行不恰当篡改，保持信息内、外部表示的一致性；可用性（Availability），即确保授权用户或实体对信息

〔收稿日期〕 2016 - 06 - 12

〔基金项目〕 孟晓阳，高级工程师，发表论文 10 余篇；通讯作者：朱卫国。

〔基金项目〕 数字化医疗医院流程研究及应用示范（项目编号：2012AA02A613）。

及资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息及资源。

医院信息系统是医院的综合枢纽，是支持医院日常运行不可或缺的一部分，但随着医院信息系统覆盖的范围越来越广，信息系统中长期累积下来的数据越来越多，对于数据安全性的要求也越来越高，使得医院信息系统中存在的安全问题开始凸显出来。在医院信息化建设中，虽然各家医院也都将信息系统安全作为信息化建设的内容之一，但是其关注重点主要集中在数据完整性和高可用性方面，如数据备份、异地双活等；对保密性的防护还仅基于制度层面，在技术层面即使投入了一些安全设备，但应用状况也并不理想。

近年来，随着互联网的飞速发展和“互联网 +”在医疗领域的广泛尝试，医院信息系统不得不由原来封闭的、隔离的园区网络系统向开放的互联网体系融合。如何防范对医院信息系统的入侵和数据窃取成为需要探讨的问题。本文从技术角度出发，通过分析已经公开的安全事件案例，了解其经验教训，结合当前医疗 IT 领域存在的普遍问题，探讨“互联网 +”时代医院信息系统面临的安全挑战与应对措施。

2 案例分析

2.1 国内案例

信息安全事件的发生一直伴随着信息技术的发展，且信息化程度越高的领域，信息安全事件造成的危害就越大。如 2005 年 UT 斯达康资深软件研发工程师程稚瀚通过西藏移动的内网入侵到北京移动充值中心数据库，通过激活已经使用过的充值卡，复制出了 14 000 个充值密码，获利 380 万元[4]。医疗数据包括患者个人隐私，由此产生的经济利益一直被某些不法分子所觊觎。如 2011 年福州某三甲医院发现每隔 1 个月左右就会有人在数据库上进行大处方查询，通过网络技术定位抓获了窃取信息的人员，经警方调查后发现都是前医院信息系统设计公司或相关的人员，他们熟悉数据库结构，掌握数据库的密码，受经济利益的诱惑，采用信息技术手段达到“统方”的目的[5]。

2.2 国外案例

对于患者个人隐私安全的保护，美国在《健康保险便利及责任法案》（Health Insurance Portability and Accountability Act，HIPPA）中有明确的规定，违反者会受到严厉的惩罚。如 2012 年 3 月，犹他州卫生部门一台包含个人健康信息的服务器持续受到黑客攻击，这台服务器上存储着包括患者地址、出生日期、社会保障号码、疾病诊断代码、身份号码、收费单编码和纳税人识别号码等各类信息。发现问题后，技术部门立即关闭这台服务器，但此时信息泄漏已有 1 个月了。每位受害者因此获得了 1 年的免费信用监控和身份盗用险作为补偿[6]。

3 安全挑战

3.1 非军事区（Demilitarized Zone，DMZ）

DMZ 区是为了解决外部网络访问内部网络服务器但又不允许直接访问的问题，而设立的一个非安全系统与安全系统之间的缓冲区，常用于部署 FTP、E－Mail、网站等允许外部访问的服务器，通过隔离外部网路对内网的直接访问达到内外网相对分离的目的[7]。在 DMZ 区与外网、DMZ 区均设有防火墙，常见的配置策略是 IP 地址级的，即防火墙对于外网的访问请求与提供对应服务的主机 IP 地址进行映射，但通常不对访问的协议进行限制，见图 1。如果此区域内主机防护薄弱，则很容易被黑客远程控制，以此作为跳板进一步入侵到内网。

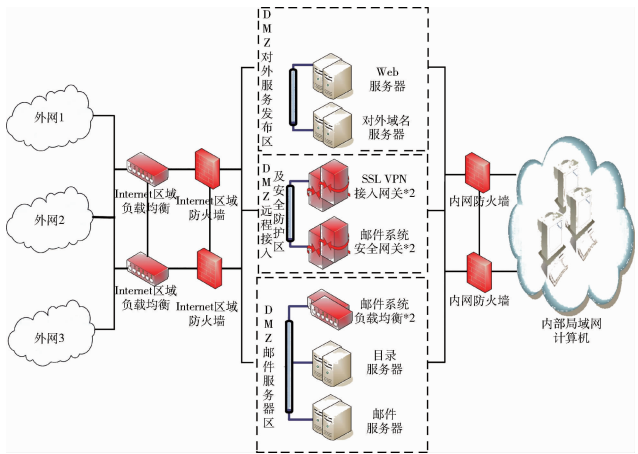

图 1 DMZ 区部署示意

3.2 虚拟专用网络(Virtual Private Network，VPN)

VPN 是指在公用网络上建立专用网络，进行加密通讯，在企业网络中有广泛应用。VPN 网关通过对数据包的加密和数据包目标地址的转换实现远程访问。VPN 有多种分类方式，主要是按协议进行分类，VPN 可通过服务器、硬件、软件等方式实现[8]。基于信息系统远程维护和用户远程访问内网资源的需要，目前很多医院建立了基于 VPN 技术的外网访问内网的通路，但如果用户密码强度较低或疏于管理，一旦被潜在入侵者窃取，即存在被仿冒远程进入医院内网环境的风险；之后入侵者可利用所获取的权限，远程控制、攻击医院内部的信息系统。

3.3 无线局域网

无线局域网具有空间覆盖范围大、不受网线束缚的优点，但同时也对安全管理提出了新的挑战。与有线局域网不同，网络管理员无法通过物理线缆的连接定位终端设备的物理位置；由于其覆盖范围大，医院院墙之外也可搜索到院内网的无线信号；特别是如“360 随身 wifi”之类的终端计算机无线网络分享，很难在网络安全策略上予以禁止。

3.4 专网专线

除了医院内网与互联网的互联外，还有一类是通过专网专线的方式与医院内网交换数据的，如医保网、银医卡、114 挂号平台等，近年来此类专网专线越来越多，数据对接方式复杂。另外，此类网络本身就是为了批量传输数据设计的，数据内容集中且敏感性高，从当前系统接口设计来看，采取文件交互方式的比较多，且没有加密手段，存在风险。

4 应对措施

4.1 DMZ 区

针对 DMZ 区存在的风险，在网络层面可按“内网可以访问外网，外网不能访问内网；内网可以访问 DMZ 区，外网受控访问 DMZ 区；DMZ 区受控访问内网，DMZ 区内部逻辑隔离”的原则设置防火墙安全策略[7]，将防火墙安全策略的粒度由“IP 地址限制”提高到“IP 地址 + 端口限制”。原则上不开放 FTP、远程桌面等高风险端口。对于 DMZ 区内的主机，应按照统一的安全基线进行安装配置，明确界定软硬件厂商的工作界面，共同做好主机安全加固。对于 DMZ 区所采用的安全产品，应选择技术能力强、被广泛使用的大品牌产品，及时更新设备版本，避免因安全产品本身漏洞造成的安全风险。同时要加强日常管理，建立白名单机制，定期核对 DMZ 主机的责任人和联系方式，开展安全教育，提高用户安全知识和意识。

4.2 VPN

对于 VPN 的管理也应从技术和管理两个角度入手。从技术上首先应强制用户定期更改密码，设置密码错误多次锁定账户的策略，禁止使用初始密码，对密码长度和强度进行限制。长期来看还可考虑配置动态口令验证设备，对用户登录采取双因素认证。从管理上应将 VPN 分为办公使用和系统维护使用两类：办公使用的账户只能访问院内网门户、OA 和邮件系统；系统维护账户严格限定其可访问的逻辑区域，原则上按需开放，及时关闭。

4.3 无线局域网

无线局域网可以分为内网无线网和外网无线网两类：内网无线主要部署在业务区域，应采取严格的准入机制，如对接入设备进行 MAC 地址绑定，明确设备的用途、可访问范围和管理人，定期清查设备；外网无线主要部署在办公区域，只能访问互联网、院内网门户、OA 和邮件系统，与业务内网严格隔离。在管理上要强调严禁私接网络设备、严禁同时连接内网和外网，通过禁用内网 USB 口的方式，阻断本机无线分享的可能，同时也避免了内网数据通过存储介质流出。

4.4 专网专线

对于专网专线，相对互联网安全，但也要避免因对方网络失控造成我方网络被入侵。专网专线原

则上可以按介于可控网络与不可控网络的中间区域对待，策略配置参照 DMZ 区。从应用系统角度，也应建议相关软件厂商进行加密处理。

5 结语

医疗行业将不可避免地走向“互联网 +”的时代，从简单的收费系统到临床大数据，越来越多的医院业务依托于信息技术运行。而医院信息系统显然还没有为此做好充足的准备。正如有关信息安全专家所说：“当前医疗行业采取的安全防护手段，与其所掌握的数据资源不匹配。”有专家认为当前国内医院的信息化安全投入与国际通常的比例相差 1 ~ 2 个数量级。本文所关注的安全边界控制问题只是安全防护的第 1 道关口，一个安全的信息系统还应建立更加完善的纵深防御体系，包括主机配置的安全基线、按应用系统划分的网络域隔离、数据加密传输存储、用户行为监控与审计等，最终达到进不来、拿不走、看不懂、改不了、走不脱、有记录的网络信息安全建设目标。

参考文献

1 何玲，刘曰波，魏津瑜. 信息安全四十年三大步［J］. 信息系统工程，2007，(12)：64 - 65.

2 李亚子，尤斌，王晖，等. 医疗保险信息泄露案例分析及对我国安全隐私保护的借鉴［J］. 医学信息学杂志，2014，35 (2)：6 - 12

3 孟晓阳，郭杰峰. 使用 IT 运行监控系统保障医院信息系统的高可用性［J］. 医学信息学杂志，2015，36 (2)：23 - 26.

4 IT 治理俱乐部. 对程稚瀚案的分析［EB/OL］.［2016 - 01 - 10］. http：//blog. vsharing. com/itgov/A884579. html.

5 赵韡. 赵韡：医院信息安全威胁案例及应对方法［EB/OL］.［2016 - 01 - 10］. http：//news. hc3i. cn/art/201411/31752. htm.

6 McCann E. Slideshow：10 biggest HIPAA data breaches in the U. S［EB/OL］.［2016 - 01 - 10］. http：//www. he-althcareitnews. com/slideshow/slideshow - 10 - biggest - hipaa - data - breaches - us.

7 陈卫平. DMZ 区安全建设模型初探［J］. 现代电视技术，2013，(2)：125 - 128.

8 百度百科. VPN 虚拟专网［EB/OL］.［2016 - 01 - 10］. http：//baike. baidu. com/link？ url = LUtKs9S9gNTbYvYu2hvR9dNLrs4NHeEcn8bpS2 - JJh3mm4vs4Dusnluzoe4pxXny1wyQ7tyVWxo3OOKlWmKxLa.

9 张益钊，朱卫国，孟晓阳，等. 医院信息系统等级保护测评实践［J］. 医学信息学杂志，2015，36 (10)：14 - 18.

(上接第 17 页)

11 李准，冯思佳，杨美洁，等. 关联规则技术在冠心病电子病历中的应用［J］. 医学信息学杂志，2015，36 (1)：58 - 62.

12 Wu X，Zhan F B，Zhang K，et al. Application of a Two - step Cluster Analysis and the Apriori Algorithm to Classify the Deformation States of Two Typical Colluvial Landslides in the Three Gorges，China［J］. Environmental Earth Sciences，2016，75 (2)：1 - 16.

13 施卓敏，孙健英，何晓涛. 基于两步聚类分析方法的 ARP 系统用户分析［J］. 计算机与现代化，2014，(3)：73 - 76.

14 Zhang T，Ramakrishnan R，Livny M. BIRCH：an efficient data clustering method for very large databases［J］. ACM Sigmod Record，1996，25 (2)：103 - 114.

15 杨遇春，林志国，戴钦舜，等. 高血压脑出血及脑梗塞危险因素 Logistic 回归分析［J］. 中国慢性病预防与控制，1995，3 (1)：3 - 6，46.

16 刘湘琳，吕淑荣，张凤云，等. 高血压合并糖尿病的相关危险因素分析［J］. 南京医科大学学报：自然科学版，2013，33 (1)：68 - 72.

17 孙静，黄玉艳，吴雷，等. 糖尿病人群高血压的发病率及影响因素［J］. 中华高血压杂志，2013，21 (7)：654 - 658.

18 霍勇，付洪喜，金振刚，等. 高血压伴冠状动脉粥样硬化性心脏病患者降压治疗的选择［J］. 中华高血压杂志，2011，19 (4)：305 - 311.

19 刘爱兵，李俊锋，卢艳芬. 对难治性高血压患者在不同性别及年龄中病因构成的探究［J］. 当代医学，2013，19 (19)：47 - 48.