医院与 CDC 信息交换的安全域设计

陆 晶 刘 立

（河北省唐山市路北区疾病预防控制中心 唐山 063000） （华为赛门铁克科技有限公司 北京 100034）

〔摘要〕 全国卫生信息系统正在加速统一整合，医院信息系统从封闭走向开放，安全问题日益突出。介绍安全域划分的目的、依据、原则及等级防护，具体探讨医院信息系统与 CDC 进行信息交换时医院信息系统的安全域模型的设计，并强调安全域管理保障的重要性。

〔关键词〕 CDC；安全域；数据交换

Security Domain Design of Information Exchange between Hospitals and Center for Disease Control and Prevention *LU Jing*, *Center for Disease Control and Prevention*, *Lubei District of Tangshan City*, *Hebei Province*, *Tangshan 063000*, *China*; *LIU Li*, *Huawei Symantec Technologies Co., Ltd.*, *Beijing 100034*, *China*

〔**Abstract**〕 National health information system is accelerating its integration, hospital information systems (HIS) are stepping from a closed period into an open era. Security issues are increasingly pop out. The paper introduces the aim, the basis, the principle and the level protection concept in the partition of security domain, concretely discussed the design of security domain when information exchanged happened between HIS and center for disease control and prevention (CDC), meanwhile emphasized the significance of the security management.

〔**Keywords**〕 CDC; Security domain; Data exchange

1 引言

《中共中央 国务院关于深化医药卫生体制改革的意见》（中发〔2009〕6 号）要求加快医疗卫生信息系统建设，完善以疾病控制网络为主体的公共卫生信息系统，提高预测预警和分析报告能力。再次对疾病预防控制中心（CDC）的信息化能力提出了期望。CDC 要实现该目标，需要广泛而快捷地收集数据，其中，与全国各类医院的信息交互，是收集数据的重要组成部分。

〔收稿日期〕 2009－12－03

〔作者简介〕 陆晶，主管医师。

不同的医院信息化程度不一，各自拥有不同的软件应用系统和硬件环境。当这些医院信息系统从封闭走向与 CDC 的开放对接，增加了新的系统外部接口，系统边界发生变化。其原有的安全动态平衡被打破，带来新的安全风险和威胁。通过安全域，分清边界，分区隔离，实现针对性分级防护，是医院信息系统和 CDC 交互数据情况下解决安全问题的基础。

2 安全域划分的目的、依据、原则、等级防护

2.1 安全域划分的目的

安全域划分的根本目的是把一个大规模复杂系统的安全问题化解为更小区域的简单系统的安全保护问题，它是对大规模复杂信息系统实施安全保护

的有效方法[1]。面对一个互联、复杂的信息系统，单独对每项信息资产确定保护方法，是非常复杂繁琐的工作，通常会因为疏忽或错误，出现安全漏洞。将整个系统当成一个安全等级来防护，也难免造成没有防范层次和防范重点，会对风险尤其是内部风险的控制不足。为了解决这个矛盾，面对复杂的信息系统，可进行安全域的划分。通过安全域的划分，对系统、风险、安全需求进行分析、修正，明确防护需求，建立组网原则；结合业务系统，跟踪特定环境的变化，进行持续需求的再分析，调整适当保护，建立持续保障机制；帮助设计防护机制的强度，保护等级，并评估和监控安全防护的力度，进行等级保护，建立评估与监控机制；针对特定环境确定安全产品、技术的部署原则，有效防护，清晰边界。安全域划分是安全防护的基础，着重于分清资产防护界限，识别各区域威胁，分区隔离保护，从而实现针对性的分级别分层次防护[2]。

2.2 安全域划分的理论依据

要实施安全域的划分，需要先充分评估医院信息系统的安全风险。通常，安全域的划分主要遵从技术、管理和过程 3 个方面的理论。（1）信息安全技术方面：遵从国际、国内和卫生行业性法规，例如 GB18336 idt ISO/IEC15408 信息技术安全性评估准则，IATF 信息保障技术框架，GB17859 计算机信息系统安全等级划分准则等；（2）信息安全管理方面：遵从 BS7799，ISO/IEC 13335，ISO/IEC 17799，COBIT 等信息安全管理实践准则；（3）信息安全过程方面：遵从 ISSE 信息系统安全工程，SSE－CMM 信息安全工程能力成熟度模型等。

2.3 安全域划分的原则

在划分安全域时，可从物理和逻辑的两个维度来进行考虑：一是从管理组织架构及物理资产管理维度来划分物理边界；二是从业务数据访问流程所依赖的 IT 架构逻辑来划分，建立 IT 管理逻辑边界。在实际操作中，安全域的划分遵从：（1）信息资产价值相近原则；（2）面临的风险相似原则；（3）安全域是整体安全体系建设中的一环，安全域的划分应满足安全体系整体的要求；（4）安全域的划分必须有较强的可实施性，能够与现有系统结合，平滑过渡，并保障设计的扩展性。

同时在划分的时候要考虑以下两个方面：（1）安全域的划分和业务紧密联系的矛盾：在安全域划分时会面临有些业务紧密相连，但是根据安全要求（信息密级要求，访问应用要求等）又要将其划分到不同安全域的矛盾，是将业务按安全域的要求强性划分，还是合并安全域以满足业务要求，必须综合考虑业务隔离的难度和合并安全域的风险（会出现有些资产保护级别不够），从而给出合适的安全域划分；（2）安全域划分数量和资产保护需求的矛盾：一般来说，将安全域划分越细，对于资产的保护会更好，但是安全域划分越细，也会带来操作上的复杂性和更多的人力投入，应对资产的保护以及划分安全域的力度进行合理取舍，一个安全域的保护要求不应该离域中所有要保护资产的要求太远。

2.4 安全域的等级防护

安全域划分之后，下一步就是建立安全域的等级防护。安全域等级防护的作用是根据安全需求确定所需的安全服务，建立适当强度的安全机制以及评价机制。这里涉及 3 个概念：（1）安全域等级：取决于系统重要程度即资产价值，资产价值高的系统，相应的安全域等级也高；（2）安全域防护等级：由安全域的资产价值和风险环境决定，资产价值高且风险高的系统，安全域防护等级相应就高；（3）安全域间的信任等级：根据安全域之间的资产关系、访问关系以及特定的风险来源分析，确定两个安全域间的信任关系和等级。

这里提到的资产价值，主要体现在业务系统的价值，需要考虑企业业务活动对业务系统的要求以及业务系统所需完成的任务；业务系统和数据的关键程度，对业务的影响程度；业务系统和数据的保密性、完整性及可靠性要求；资产之间依赖关系等因素。风险环境决定了面临的风险，需要考虑用户的组成和分布，系统内、外部连接，风险的可能来源和动机、可能性、影响等因素。

3 医院与 CDC 互联的安全域划分

3.1 安全域划分

医院信息系统与 CDC 互联，IT 物理架构和业务流程都发生了变化[3]，原来单一的信息系统变成 4 部分：用于连接 CDC 的接口区，为 CDC 提供 VPN 服务和数据交换服务的对外服务区，访问 CDC 业务的用户区以及和 CDC 不发生直接关系的业务区。因此，从 IT 物理架构和业务流程的二维角度，医院信息系统的安全域划分模型，见图 1。

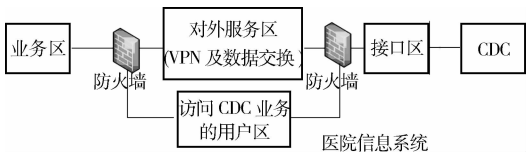

图 1 医院信息系统的安全域划分模型

（1）接口区：提供连通性服务，它是医院信息系统的出口，用于连接 CDC，通常接口部署一台路由器，是外部进入医院信息系统的入口，受到的安全威胁最大，但它本身没有数据，仅提供连通性服务，受到安全攻击后，只造成服务不可用，与 CDC 数据交换中断，不会产生数据泄密等问题；（2）对外服务区：为 CDC 提供 VPN 和数据交换服务，是医院信息系统与 CDC 进行数据交换的核心[4]，该区域部署 VPN 设备和数据交换服务器，只与特定的 CDC 系统通信，受到的安全威胁较小，但受到安全攻击后，一方面数据交换服务不可用，另外，还会产生数据泄密问题；（3）访问 CDC 业务的用户区：该区的用户需要同时访问 CDC 业务和医院业务系统，因此，需要对用户行为进行控制，加强安全措施，避免有意或无意的安全问题威胁 CDC 业务和医院业务系统；（4）业务区：是医院信息系统的核心区域，具有核心的业务系统和核心的数据，一旦被攻击不但影响医院的业务开展，也会导致数据泄密、篡改和删除。

3.2 各安全域访问关系

4 个区域之间需要隔离和控制，通过部署防火墙来实现。防火墙的本质功能就是隔离网络，通过防火墙可以把普通区域、重点区域等各种逻辑网络进行隔离，避免不安全因素扩散[5]。灵活的网络隔离特性是防火墙非常重要的一个特性，只有在各安全域边界合理利用这些特性，各安全域的受信访问才可以得到保障，安全策略才可以更有效地实施。

（1）对外服务区与接口区：对外服务区通过接口区与 CDC 双向通信，即特定的 IP 地址、端口与特定的 IP 地址、端口通信；（2）业务区与对外服务区：双向通信，同样是特定的 IP 地址、端口与特定的 IP 地址、端口通信；（3）对外服务区与访问 CDC 业务的用户区：当用户区需要通过 VPN 访问 CDC 时，依次通过对外服务区和接口区，这种访问为单向访问，由用户区发起，且为用户对 CDC 特定 IP 和端口的访问；（4）接口区与访问 CDC 业务用户区：当用户不需要通过 VPN 访问 CDC 时，通过接口区进行，同样为单向访问；（5）业务区与访问 CDC 业务的用户区：由用户区发起，对业务区的单向访问，是用户对业务区特定 IP 和端口的访问。各安全域之间访问规则，见图 2。

3.3 各安全域防御策略

（1）接口区：主要是对用于外联的网络设备进行 DOS 防护和防止源路由攻击，拒绝服务攻击——通过恶意消耗资源，来阻止合法用户对资源的访问，比如通过发送大量报文使得网络带宽资源被消耗或者采用大量的 ping 等手段，消耗设备处理能力，源路由攻击 —— 报文发送方通过在 IP 报文的 Option 域中指定该报文的路由，使报文有可能被发往受保护的医院信息系统；（2）对外服务区和业务区：主要是确认身份，检测入侵，控制行为以及防御对服务的 DOS 攻击等，身份确认——确认访问该区域的用户的身份是合法的，身份的确认可以通过 IP、端口、用户名、密码等各类方式，入侵检测——主动侦听该安全域中是否存在恶意攻击、入侵或其他安全隐患行为，行为控制——控制合法用户的行为，避免不合规定的无意或恶意操作；（3）访问 CDC 业务的用户区：确认身份，检测入侵，控制行为，防护终端等，身份确认——建立认证系统，

确保该区的用户身份均合法，终端防护——即终端安全，确保用户操作终端安全、可控，没有漏洞、木马、病毒等一系列潜在安全威胁。

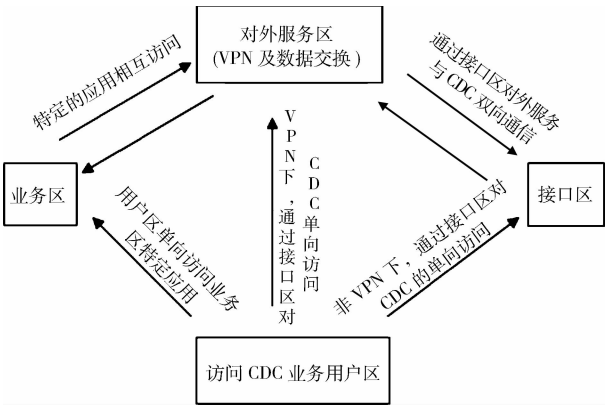

图 2 各安全域之间访问规则

4 安全域的管理保障

“三分技术，七分管理”[6]，确保医院与 CDC 互联下 IT 系统的安全，采用单纯的技术手段是远远不够的，必须依靠必要的管理手段和安全建设方法论来支持。通过合理的组织体系、规章制度和管理措施，把具有信息安全保障功能的软硬件设施和管理、使用信息的人整合在一起，以此确保整个组织达到预定程度的信息安全，称为信息安全管理体系（ISMS：Information Security Management System）[7]。这是组织在整体或特定范围内建立的信息安全方针和目标以及完成这些目标所用的方法和体系，是基于某些被广泛承认和验证的信息安全标准和最佳实践，例如 ISO27001、ISO17799 等，建立起来的信息安全管理体系。

建立一个有效的信息安全保障体系，首先是确定信息安全的策略和范围，然后在风险分析的基础上选择适宜的控制目标和控制方式，最后制定业务持续性计划，建设实施信息安全体系。ISMS 的保护对象其实就是医院信息安全最终对应的元素，其中人员和数据是两个对象，而资产则是一个媒介。最终可达到的保护效果就是：进不来、拿不走、看不懂、改不了、毁不掉、逃不了。在医院的信息系统安全管理方面，可将 PDCA（Plan，Do，Check 和 Act）持续改进的信息安全风险管理模型贯穿整个医院信息系统生命过程。PDCA 模型主要过程是：在计划（Plan）阶段通过风险评估来了解安全需求，建立全面的安全标准和制度体系；在实施（Do）阶段将遵照标准和制度体系执行和落实安全控制措施；在检查（Check）阶段监视和审查安全控制的执行情况，并跟踪系统环境变化；在改进（Act）阶段维护改进安全标准和制度体系。以风险管理为基础，通过建立一整套文件化的管理制度，包括方针、策略、程序文件，操作手册、记录等，在医院中以 PDCA 的方式实施，把风险控制在医院可接受的水平。

5 结语

医院信息系统除了与 CDC 连接外，还与卫生监督、妇幼保健、精神病防治、新农合、医院、医保、民政、公安、残联、体检中心等系统连接，进行数据交换。在与这些系统进行互联时，均可借鉴上述安全域划分模型，建立基础安全架构。同时各医院可以用安全域划分的原则和方法，划分更细致、更符合自身需求的安全域，并在 ISMS 的框架下，构建安全性强的医院信息系统。

参考文献

1 于慧龙，李萍. 大型信息系统安全域划分和等级保护〔J〕. 计算机安全，2006，(7)：11－12.
2 向宏，艾鹏，刘嘉伟. 电子政务系统安全域的划分与等级保护〔J〕. 重庆工学院学报（自然科学版），2008，(2)：105－109.
3 中国疾病控制预防中心. 国家传染病和死亡网络直报系统与医院信息系统连接相关技术指导方案〔Z〕. 2008
4 杨宏桥，吴飞，刘玉树. 安全数据交换技术在 HIS 中的应用〔J〕. 计算机工程，2008，(22)：201－203.
5 刘建伟，王育民. 网络安全——技术与实践〔M〕. 北京：清华大学出版社，2005.
6 蒋朝惠，许石青. 我国信息安全管理的现状、问题及对策〔J〕. 信息化建设，2005，(4)：46－49.
7 姚轶崭，江常青，张利，等. ISMS 概念模型探索〔J〕. 计算机工程，2008，(2)：139－140，152.