电子病历信息安全共享关键技术①

高 敏, 叶 晰, 蒋 静, 周万里, 张 凯

(温州医学院 信息与工程学院, 温州 325035)

摘 要: 电子病历作为电子医疗信息的重要组成部分, 其推广应用的主要问题之一是如何方便快捷的共享各种电子病历信息, 同时又保护好患者的隐私. 首先分析了当前电子病历信息共享所面临的各种安全问题, 介绍了动态口令技术的基本原理和技术模式, 研究和开发了一种基于动态口令的访问控制体系. 动态口令(或称一次性密码)根据用户的安全级别和实用性要求, 可以分别用软件, 手机或者电子令牌产生. 该身份认证技术可以与现存的各种医院信息系统无缝融合, 这样一来既保证了电子病历信息安全、快捷和方便地共享, 又能保护患者的隐私不被非法用户和黑客所窃取.

关键词: 电子病历; 安全共享; 动态口令; 手机令牌

Key Technology of Sharing Computer-Based Patient Record Safely

GAO Min, YE Xi, JIANG Jing, ZHOU Wan-Li, ZHANG Kai

(School of Information and Engineering, Wenzhou Medical College, Wenzhou 325035, China)

Abstract: Computer-based patient record is the most important part of electronic medical information. The main problem for applying computer-based patient record is how to share patient information safely and protect patient privacy in the meantime. In this article, the safe sharing issues of computer-based patient record are described. The principle of dynamic password is described and an access control system based on dynamic password is designed. Dynamic password (one time password) can be produced by software, mobile phone and electric token according to the user safety level and different request of user. This identity authentication system based on dynamic password can be easily merged into most of hospital information systems. By using this technology, computer-based patient record can be shared by different organizations safely, quickly and conveniently. In the meantime, the patient privacy can be protected very well also.

Key words: computer-based patient record; safe sharing; dynamic password; mobile phone token

建立和推广居民健康档案和电子病历, 是新医改背景下我国医药卫生信息化建设的重点[1]. 目前在病人转诊的过程中, 医院与社区卫生院作为不同级别的医疗机构, 相互之间并没有共享患者的疾病治疗过程和就诊信息等情况. 不必要的复查导致医疗服务效率降低和患者医疗费用的增加. 建立区域性的统一的电子医疗信息共享平台, 能降低病人的诊疗费用, 为医生的诊疗工作提供更详尽的参考作用, 并使上级医院对下级医院的诊疗产生一个良好的指导性作用[2]. 可以说, 电子病历和居民健康档案等电子医疗信息的共享是信息技术和网络技术在医疗领域的必然产物, 是医院医疗信息现代化管理的必然趋势[3]. 在目前医患纠纷频发的背景下, 患者对于个人医疗信息的知情权诉求更加强烈, 所以医疗信息在医院和患者以及院际之间的共享成为必然趋势. 同时由于个人电子病历信息涉及到诸多个人隐私, 如何保护这些信息不被窃取也成为一个非常迫切的研究课题.

① 基金项目:浙江省大学生科技创新计划(新苗人才计划)项目(2012R413026);浙江省教育厅科技项目(Y201222952);温州市科技局科技项目(Y20100301).

通讯作者: 叶晰 E-mail：JamesXiYe@163.com

收稿时间:2012-04-14;收到修改稿时间:2012-05-14

1 电子病历信息共享的形式和面临的问题

由于电子病历储存了有关患者个人的基本情况、健康状况、疾病发展、诊疗情况等信息, 使得电子病历和传统病历一样包含了大量的病人隐私. 电子病历的形成、保存和利用与传统纸质病历相比有其自身的优势和特点, 也使患者隐私权保护出现了新的变化[4]. 电子病历信息共享的主要形式包括:

① 同一医院不同医生共享同一个患者的医疗信息.

② 不同医院共享患者的医疗信息(可能通过专用的医院网).

③ 社区卫生服务中心和医院之间的医疗信息共享(可能通过因特网).

④ 法律赋予了患者对自己整个医疗过程的知情权, 所以在医患纠纷频发的当今社会, 患者必须能方便快捷真实的看到自己的医疗信息(通过因特网).

根据以上几种电子病历信息共享的形式, 电子病历信息共享中面临的安全隐患包括:

① 医院信息系统本身存在安全隐患. 所有在医院局域网内的计算机使用人员都可能是信息的窃取者.

② 不同的医院之间电子病历信息的共享要通过因特网(或者专门的医院网), 而这些在外部计算机网络中传播的信息很容易被黑客所拦截和窃取, 从而造成患者个人隐私的泄漏.

③ 医院信息系统内部管理不规范. 主要包括访问权限管理的不规范等, 造成低权限的人可以越级阅读或修改患者的电子病历信息.

电子病历信息共享的形式和传播途径的多样性也决定了安全隐患的多样性, 所以如何针对不同的安全隐患而提出不同的解决方案是本系统的要解决的主要问题之一.

2 动态口令的基本原理和技术模式

2.1 动态口令技术的基本原理

动态口令又称为一次性口令(OTP: One Time Password), 其特点是用户根据服务商提供的动态口令令牌的显示数字来输入动态口令, 而且每个登录服务器的口令只使用一次, 窃听者无法用窃听到的登录口令来做下一次登录, 同时利用单向散列函数(如 SHA-1 算法等)的不可逆性, 防止窃听者从窃听到的登录口令推出下一次登录口令[5]. 选取动态口令认证这种方案的商用系统采用的是静态密码与令牌相结合的方式进行身份鉴别. 这种方式在检查用户静态密码(知道什么)的同时, 验证用户是否持有正确的令牌(拥有什么)[6].

2.2 动态口令技术模式的选择

根据不确定因素的选择方式, 动态口令可以分为: 时间同步机制、事件同步机制和挑战/应答机制, 其特点如下[7]:

(1) 基于时间同步的令牌, 一般每 60 秒产生一个新口令, 但由于其同步的基础是国际标准时间, 故要求其服务器能够十分精确的保持正确的时钟, 同时对其令牌的晶振频率有严格的要求, 以降低系统失去同步的几率.

(2) 基于事件同步的令牌, 其原理是通过某一特定的事件次序及相同的种子值作为输入, 在算法中运算出一致的密码. 由于其算法的一致性, 其口令是预先可知的, 通过令牌, 你可以预先知道今后的多个密码. 同样, 基于事件同步的令牌也存在失去同步的风险.

(3) 基于挑战/应答模式的令牌属于异步令牌, 由于在令牌和服务器之间除相同的算法外没有需要进行同步的要求, 故能够有效的解决令牌失步的问题, 降低对应用的影响, 同时极大的增加了系统的可靠性. 异步口令使用的缺点主要是在使用时, 用户需多一个输入挑战值的步骤, 对于操作人员, 增加了复杂度.

基于时间同步的令牌技术实现比较容易, 且无需额外输入, 客户满意度较高, 故我们最终采用基于时间同步的令牌技术.

3 系统算法设计和实现

3.1 生成动态口令的算法

动态口令的产生和验证过程如图 1 所示. 为了方便描述, 对图中采用的符号做如下定义: A 为用户; S 为认证服务器; ID_A 为 A 的标识; K_{A1} 为 A 用户密钥 1; K_{A2} 为 A 用户密钥 2; P_A 为动态口令; T 为时钟计时器.

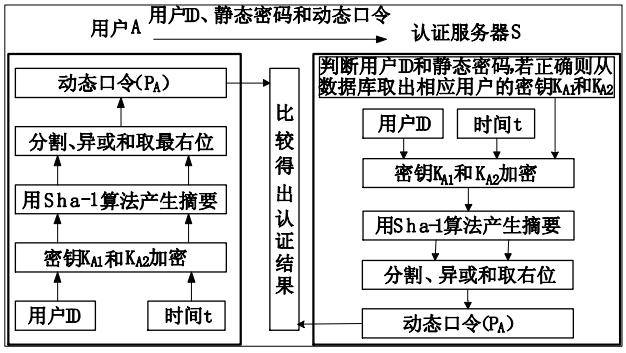

图 1 动态口令的产生和验证流程图

客户端软件保存有用户 ID 号和密钥信息，用户密钥 K_{A1} 和 K_{A2} 在用户注册时随机产生，保存在认证服务器端的用户注册信息表中. 软件中的时钟计数器 T 每隔 60 秒自动用密钥 K_{A1} 和 K_{A2} 同时加密用户 ID 和当前时间 t(精确到分钟)，然后用 Sha-1 算法对加密结果进行单向散列计算(相当于第二层加密)，产生两个等长的 40 位十六进制摘要. 如用户 ID=“19760130”，K_{A1}=12，K_{A2}=25，经过加密得出 40 位的摘要为“233dacc7000d300efcbb8feaca7533ce1a0a1440”；同样的方法对当前时间进行加密得出摘要为“26e654ba40d68c6a4b806708a3fc0c5683eddf9b”. 把这两个摘要分别平均分割为 8 段并转换为十进制，最后把两组 8 段的十进制数分别进行异或运算并取每段最右边位得到最终的 8 位动态口令(如本例中为：“9 2 8 1 4 9 4 9”).

3.2 动态口令的验证

验证服务器收到用户输入的用户 ID、静态密码和动态口令后，先验证用户 ID 和静态密码是否正确，如正确则在数据库中读出该用户的密钥 K_{A1} 和 K_{A2}. 这两个密钥在发布动态口令客户端软件时应该已确定，并存放在验证服务器端的数据库内. 使用密钥 K_{A1} 和 K_{A2} 对用户 ID 和当前时间 t 进行同客户端相同的处理，最终产生验证服务器端的动态口令，并与客户端传来的动态口令进行比较，一致则通过验证.

3.3 客户端产生动态口令的三种载体

由于对电子病历信息进行共享的主体不一样，其学习能力和成本承受能力也不一样. 如本医院的医务人员需要随时都能快捷的共享病人的电子病历信息，而且其身处相对安全局域网内部，所以我们可以把身份认证软件做成网页浏览器的插件，以便医务人员快捷方便的访问医疗信息. 而对于院际之间的电子病历信息远程共享，由于可能要经过相对不安全的因特网，我们可以提高安全级别，采用安全性和成本都比较高的电子口令牌等来实现身份认证. 对于一般患者，我们可以采用相对廉价的基于手机的动态口令牌或者口令卡等来实现身份认证. 下面我们分别描述一下这三种实现方法.

3.3.1 网页插件形式

首先我们用 C#语言完成客户端软件的编写，然后在 Microsoft Visual Studio 2008 平台下转换为 AxtiveX 控件并发布给用户. 每个 AxtiveX 控件都包含有该用户的 ID 和密钥，控件发布可通过用户注册时直接下载或发到用户信箱等方式. 其具体运行效果如图 2.

图 2　ActiveX 控件运行效果图

3.3.2 手机令牌形式

手机程序运行的几种主流平台包括[8]:

1) Java 2 Micro Edition (J2ME)

2) Apple IOS

3) Symbian

4) Android

5) Windows Mobile Smartphone

由于 Java 语言广泛的网络支持和它的平台无关性特点，只要安装了 Java 虚拟机的手机都可以运行 Java 程序，真正实现了“一次编程，到处运行”的理念，故选择 J2ME 作为手机令牌的开发平台. 网站首先根据用户的注册信息生成一个 Java 安装文件，并发放给用户(可通过蓝牙下载、网页直接下载和短信通知等多种方式)，用户下载并安装生成手机令牌软件. 登录医院系统时，用户运行令牌软件得到相应的 8 位动态口令. 其具体运行效果如图 3.

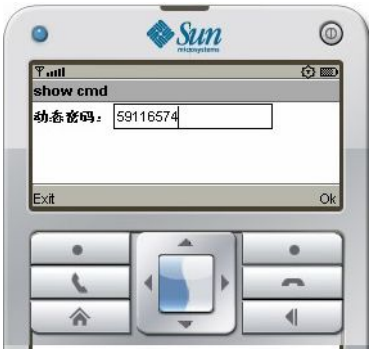

图 3　手机令牌的运行效果图

3.3.3 电子口令牌

电子口令牌(Token)的主要优点是安全性高且使用和携带方便，一个常用的电子口令牌需要解决：输入设备、输出设备、CPU、存储设备、电源、通信端口、晶振以及二进制和十进制的互相转换等诸多问题[9]，故其成本比其他两种实现方法要高很多，所以我们一般只在院际之间的远程共享电子病历信息时采用电子口令牌来实现认证.

4 系统的实施流程

动态口令系统的实施步骤为:

1) 新用户先在医院网站上注册会员，并要求提供动态口令服务.

2) 新用户通过网站审核后，网站产生两个随机整数作为该用户密钥 K_{A1} 和 K_{A2}(如 12, 25)并存放于数据库用户登录信息表中.

3) 网站根据该用户 ID(注册时产生)和其相应的密钥 K_{A1} 和 K_{A2} 生成一个口令生成文件，并发放给该用户(可采取 Active 插件下载到用户浏览器中、用户直接用手机下载手机令牌软件和电子口令牌等方式). 当用户登录网站时，必须先运行口令生成文件得到该时段(精确到分钟)的动态口令.

4) 登陆时用户在网站上输入用户 ID、静态密码和动态口令后，如果正确即可登陆成功. 登录界面如图 4 所示.

图 4 电子病历系统登录界面图

5 系统碰撞率测试

不同的明文如果经过加密后密文是一样的，则我们称这种现象为碰撞. 由于动态口令位数固定，所以碰撞是在所难免的. 窃听者在截取了大量老的动态口令后，可能组成一个口令字典，然后对认证系统进行攻击，故碰撞率的高低直接决定了动态口令系统的抗攻击性. 本程序实际应用中动态口令每分钟变一次，在测试中为了提高效率，我们让动态口令每秒变一次，测试周期最长的为 6.5 天，相当于实际应用中大约一年的时间(即 6.5×60=390 天). 其碰撞数据如表 1 所示.

表 1 碰撞数据表

用户 ID	Key1	Key2	口令数	碰撞次数	碰撞率
19760130	12	25	15786	1	0.0063%
19760130	122	255	75875	26	0.0343%
19760130	122	255	261698	356	0.1360%
19760130	18	189	565514	1574	0.2783%
95484032	43	218	565511	1556	0.2751%
63483923	119	110	565496	1571	0.2778%

从上表中我们可以看到: 动态口令软件连续运行大约 11 天(15786÷60÷24=10.9 天)可能会出现一次碰撞(即出现一次相同的动态口令)，连续运行半年则会出现大约 356 次碰撞，连续运行一年则其碰撞次数稳定在 1500 左右. 从以上数据可以看出，随着连续运行时间的增加，碰撞率有所增加，但碰撞率绝对值不高，而且实际应用中我们只是在需要登录时才会运行一下客户端文件并得到该时刻的动态口令，之后即关闭程序，而不会连续运行程序. 故实际应用中碰到相同动态口令的几率是很低的.

6 关键技术和安全性分析

6.1 时间同步问题

基于时间同步机制的动态口令系统一般每 60 秒产生一个新口令. 如果使用电子令牌的硬件实现方法，由于其同步的基础是国际标准时间，故对令牌的晶振频率有严格的要求，以降低系统失去同步的几率. 但随着时间的流逝，误差总是会出现的，当服务器和令牌的时间偏移超过一定值时，则系统验证会出错. 对于失去时间同步的电子口令牌，目前可以通过增大偏移量的技术(前后 3 分钟)来进行远程同步，确保其能够继续使用，降低对应用的影响. 而用软件实现动态口令技术，则解决时间同步问题的方法相对简单，只要定期通过校时网站(如: time.windows.com 等)校准一下服务器和客户端的系统时间即可解决同步的问题. 当然我们也可以模拟硬件实现的增大偏移量的技术来进行远程同步，如在服务器端算出前后 3 分钟的动态口令，然后与客户端传来的动态口令进行一一比对.

6.2 系统的安全性分析

(1) 本系统能有效抵抗截获重放攻击，即使攻击

者可以通过一些手段窃听到用户的动态口令, 但是由于动态口令是一次性的, 且我们限制同一账户同时只能一人在线, 故窃听到的口令即使发送给认证服务器也不能通过认证. 而且每个动态口令之间是不相关的, 不能从这个动态口令推出下一个动态口令, 所以攻击者窃取到了老的动态口令也没用.

(2) 所谓的字典攻击是指窃听者在截取了大量老的动态口令后, 可能组成一个口令字典, 然后对认证服务器进行攻击. 从上面的碰撞性测试的数据中我们得知窃听者平均连续截获了 15786 个以上动态口令后(即连续窃听 11 天以上), 再在验证服务器上连续输入这些动态口令, 才可能会有一次成功的机会. 即使窃听者做到了长时间窃听, 但我们仍可以在认证服务器端设置了账户锁定功能, 只要用户连续几次输入错误的动态口令, 则该用户即被临时锁定了. 故该认证系统可以抵抗字典攻击.

(3) 认证服务器的帐户锁定功能使得蛮力攻击和猜测攻击难以成功, 一个攻击者要在有限次数内猜中 8 位动态口令值的概率极小. 故该认证系统可以抵抗暴力破解攻击.

(4) 该系统没有实现双向认证, 故不能抵抗中间人攻击. 由于认证协议的单向性, 即服务器可以验证用户的身份, 而用户不能验证服务器的身份, 若攻击者冒充服务器(即钓鱼网站), 就可以得到用户的口令, 并可以将此口令发送到合法的认证服务器, 通过认证, 从而接入系统. 要解决这个问题, 必须采用公钥技术设计新的密码协议, 但这会增加令牌设备的计算量, 从而降低认证速度. 当用户量较大时, 还会使认证服务器产生巨大的计算负荷[10].

7 结语

电子病历推广应用的主要问题之一是如何方便快捷的共享各种电子病历信息, 同时又保护好患者的隐私. 本文阐述了一种基于动态口令的访问控制体系. 该认证技术实现的方式有很多种, 除了使用相对的昂贵电子口令牌外, 还可以用浏览器插件和手机令牌等非常廉价的方式实现, 可以为医院信息系统的安全认证节省大量购买身份认证设备的开支. 该技术可以无缝融合进现存的各种医院信息系统, 这样一来既能保证电子病历信息安全、快捷和方便的共享, 又确保了患者的隐私不被非法用户和黑客所窃取, 而电子病历信息的安全问题的解决和改善又必然进一步推进我国医药卫生信息化建设的步伐.

参考文献

1 许丽萍.尴尬的电子病历:突破知道在何方?趋势,2009,(3):36–38.
2 尤丽钰.区域性电子病历信息共享的探索和研究.科学管理,2009,(17):378.
3 孙中海,孙卫,王继伟.区域托管电子病历共享平台的构建.中国数字医学,2009,3(11):5–6.
4 马伟,许学国.电子病历共享中患者隐私权保护.卫生软科学,2009,23(3):330–332.
5 胡天麟,刘嘉勇,陈芳,隋喆.基于 MD5 的 OTP 认证系统的原理及实现.信息技术,2005,9:140–142.
6 李凤银,刘培玉,鞠宏传.OTP 技术的一种改进方案与应用.计算机系统应用,2003,12(4):34–36.
7 吴佩萱.基于时间同步机制的动态密码认证系统.长江大学学报(自然版),2005,2(7):256–257.
8 Michael Morrison,李强.J2ME 手机游戏编程入门.北京:人民邮电出版社,2005.8–10.
9 曾伟国,胡汉平,王祖喜,孔涛.基于手机令牌方式的动态身份认证系统.计算机与数字工程,2005,9:21–24.
10 Kim HC, Lee HW, Lee KS, et al. A Design of One-Time Password Mechanism using Public Key Infrastructure. Proc. of 4th International Conference on Networked Computing and Advanced Information Management. NCM 2008, 1: 18–24.