

一种确保电子病历传输安全性的模型

胡建理¹, 李小华¹, 周 斌²

(1 广州军区广州总医院信息科, 广东 广州 510010; 2 国防科学技术大学 计算机学院, 湖南 长沙 410073)

摘 要: 针对电子病历传输中的安全性问题, 提出了一种解决模型, 利用现有的安全技术充分地保障电子病历传输中的安全性. 性能分析表明, 该模型能有效地满足电子病历在传输过程中对机密性与完整性的要求.

关键词: 电子病历; 安全性; 数字签名; 加密

中图分类号: TP311.13; R197.323

文献标识码: A

文章编号: 1000-7180(2010)11-0091-03

Model for Assuring Transmission Security for Electronic Medical Record

HU Jian-li¹, LI Xiao-hua¹, ZHOU Bin²

(1 Information Department of Guangzhou General Hospital under Guangzhou Area Command, Guangzhou 510010, China;

2 School of Computer, National University of Defense Technology, Changsha 410073, China)

Abstract: With the security problems for EMR(electronic medical record) in transmission in mind, a solving model is proposed in this paper, in which, we utilize the current conventional security technologies to assure the transmission security for EMR. Performance analysis exhibits that the model can effectively cope with the security problems about confidentiality and integrity for EMR in transmission.

Key words: electronic medical record; security; digital signature; encryption

1 引言

电子病历是以电子化方式管理的有关个人终生健康状态和医疗保健行为的信息, 它可在医疗中作为主要的信息源取代纸质病历, 提供优于纸张病历的服务, 满足所有的医疗、法律和管理需求. 随着计算机和网络技术的发展, 电子病历带来了传统纸质病历所不具有的一些优点, 如病人信息查找方便快捷, 能灵活多样地显示病人信息, 有利于医疗记录的统计利用等. 但同时也带来了一些相关的安全问题, 如电子病历传输过程中如何保证其中的隐私信息不被无关的第三方查阅, 如何保证传输中的电子病历信息不被恶意的第三方破坏与非法利用等.

针对以上安全问题, 本文提出了一种确保电子

病历传输安全性的模型, 通过性能分析可知, 该模型可以有效地保证电子病历传输的安全性.

2 电子病历传输中存在的安全问题

医院电子病历系统多数运行在医院内的局域网上, 局域网上的电子病历系统终端与服务器间的信息传输安全往往被忽视, 电子病历信息在传输过程中可能被恶意的第三方截获并篡改, 其中的私密信息也可能被非授权用户获知, 因此需要采取一定的安全措施保证电子病历信息在传输中的安全性. 具体来说, 电子病历在传输中的安全性包括如下两个方面的内容^[1-2]:

(1) 信息机密性

电子病历信息直接记载着患者的临床和健康信

收稿日期: 2009-09-25; 修回日期: 2009-11-25

基金项目: 国家“九七三”重点基础研究发展规划项目基金(2005CB321800); 国家“八六三”高技术研究发展计划项目基金(2007AA010301); 国家杰出青年科学基金(60625203); 国家自然科学基金(60873204)

息,包括某些个人的隐私,因此电子病历在网络上传递的数据只允许相关人员了解,而不能够被非授权用户获知,相关用户所进行的操作在权限允许范围内属于机密信息,是不能被外泄的,许多网络攻击软件很容易就可以监听到这些机密文件,因此,信息机密性在电子病历系统中是不可忽视的安全隐患.

(2)信息完整性

信息完整性是与信息机密性非常相似的又一个安全隐患,从医护人员向病历文件服务器提交病历的那一刻起,电子病历完整性就要得到保证.电子病历在网络中传输时容易被恶意的第三方截获,通过加入或去掉其中的部分信息,甚至篡改信息来破坏电子病历的完整性,因此,必须采取相应的安全机制,防止电子病历在传输过程中随意生成、篡改和删除.

3 确保电子病历传输安全性的模型

确保移动电子病历数据传输的安全性是电子病历系统安全性的重要一环.目前各大医院对电子病历的传输安全性关注不够,我们提出的保证电子病历安全传输的方法主要是基于数据加密的方法,通过利用常规私密或公钥密码体制来保护电子病历信息在传输中的安全性,这些措施在一定程度上起到了保护电子病历信息的作用,但仍然存在着安全隐患,比如可能遭到恶意的第三方的重放攻击等安全问题等.因此,本节我们提出了一种确保电子病历传输安全性的模型,采用了一种电子病历文档完整性检测、非对称加/解密处理和时间戳机制,其具体过程如下:

为了更好地描述我们的模型,我们首先引入了一些符号参量,对其含义界定如表 1 所示.

表 1 符号说明

Symbols	Descriptions
i	发送方(医务人员)或接收方(病历服务器)
KR_i	i 的私钥
KU_i	i 的公钥
K_s	对称密钥
EP_k	用密钥 k 加密
DP_k	用密钥 k 解密
SIG_i	用 i 的私钥数字签名
H	进行 Hash 处理(报文摘要处理)
TS_i	i 生成的时间戳
$TInformation$	表示明文电子病历信息,它可代表完整的电子病历文档,也可表示电子病历中某一数据元信息,如诊断信息.

这里我们不妨设发送方为 A ,接收方为 B .发送方的具体算法如图 1 所示.

第一步, $TInformation \xrightarrow{H} H(TInformation)$, 即对明文电子病历信息作报文摘要处理,这一步既可有效地减小下一步数字签名的工作量,又可减少信道上的信息流量;

第二步, $H(TInformation) \xrightarrow{SIG} SIG_A(TS_A, H(TInformaiton))$,对第一步生成的报文摘要,及当前的时间戳信息 TS_A 用发送方的私钥 KR_A 数据签名;

第三步, $TInformation \xrightarrow{KS} EP_{K_s}(TInformation)$,对明文电子病历信息用私钥 K_s 加密,这一步可以保证电子病历信息在传输过程中的机密性,其信息对无关第三方是不可读的;

第四步, $SIG_A(TS_A, H(TInformaiton)) + EP_{K_s}(TInformation) \xrightarrow{IP} B$,将第二步生成的签名过的报文摘要信息及第三步生成的用对称密钥加密过的明文电子病历信息一起通过网络发送给病历服务器 B .

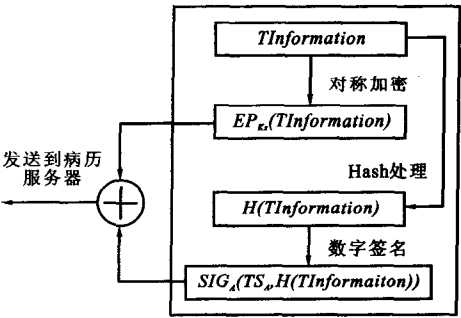


图 1 对电子病历进行安全处理过程

接收方的算法如下:

接收方将发送方传过来的信息分离,分离出加密信息与数字签名信息,并分别处理,其过程如图 2 所示.

第五步, $DP_{K_s}(EP_{K_s}(TInformation)) \xrightarrow{KS} TInformation$,将电子病历的加密信息用对称密钥解密;

第六步, $DP_A(SIG_A(TS_A, H(TInformaiton))) \xrightarrow{KS} TS_A + H(TInformaiton)$,将电子病历的数字签名信息用发送方的公钥解密,得到时间戳信息与明文电子病历的报文摘要处理信息,利用其中的时间戳信息 TS_A 可有效地防止恶意的第三方以过时的信息欺骗节点接收方的重放攻击;

第七步, $TInformation \xrightarrow{H} H(TInformation)$, 即第五步生成的明文电子病历信息作报文摘要处理;

第八步,对电子病历的数字签名信息进行验证:比较第六步与第七步生成的报文摘要信息 $H(TInformation)$,比较这两个值,可以判定明文电子病历信息在传输中是否被其他节点篡改过,或由于其他原因遭到破坏.如果两个值相等,说明电子病历信息在传输中没有被篡改或遭到破坏;反之,则需要将其抛弃,并通知发送方重发所需的信誉信息.

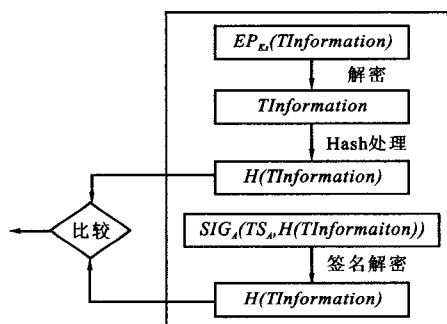


图2 完整性验证过程

4 模型性能分析

该模型综合运用了密码技术中对称密钥机制与非对称密钥机制,并利用报文摘要与数字签名技术充分保证了电子病历传输过程中的机密性与完整性.以上算法在具体实施时,为了保证电子病历信息在传输中的机密性,我们可选择高级加密标准 AES 作为对称密钥算法用于电子病历明文信息加密,这是因为 AES 加密算法^[3-5]具有运算速度快、内存需求低、算法可靠、分组长度和密钥长度设计灵活等优点.在电子病历信息中引入了上述安全机制后,为了最大限度地减少由于引入安全机制所带来的额外成本,我们采取了先对整份电子病历进行 Hash 处理,而后对所生成的报文摘要进行数字签名验证处理.利用 MD4 作为生成报文摘要的 Hash 算法,因为该算法效率很高,执行速度很快,而且目前还没有发现非常有效的攻击方法.对电子病历的报文摘要进行数字签名我们使用 ElGamal 公钥密码数字签名算法^[6],该算法的安全性主要是基于有限域 Z_p 上离散对数问题的难解性,到目前为止,还没有找到一个非常有效的多项式时间算法来计算有限域上的离散对数,它至今仍然是一个安全性能良好的公钥密码数字签名体制.为了防止恶意的第三方对接收方实

施重放攻击,该模型还引入了时间戳的概念,能较好地防止这种攻击形式的发生,从而进一步增加该模型抵御恶意攻击的健壮性.

本模型在具体应用中既能有效地保证电子病历的机密性与完整性,又能兼顾执行效率,并在一定程度上尽可能地降低引入安全机制带来的额外成本.

5 结束语

电子病历是医院信息化的必然趋势,电子病历在医院的临床医疗护理、科研教学和质量管理等方面的重要性越来越高,其安全要求也越来越高.本文重点对电子病历传输过程中的安全问题进行了系统的研究,并提出了相应的解决方案.性能分析表明,该模型可以有效地保证电子病历传输过程的机密性与完整性,同时兼顾执行效率与综合成本的平衡问题.

参考文献:

- [1] 王自力,刘仲祥,王薇,等. 医院信息系统的安全管理[J]. 中国医院管理, 2006, 26(3): 32-33.
- [2] 李华才,肖静. 电子签名技术在医疗工作中的应用与影响[J]. 医学信息, 2004, 17(1): 27-29.
- [3] 王海洋,陈弘毅. 一种小面积的高吞吐率 AES 协处理器设计[J]. 微电子学与计算机, 2009, 26(6): 12-16.
- [4] 田俊峰,毕志明,张晶. 一种基于公钥的新型 Kerberos 域间认证方案[J]. 微电子学与计算机, 2008, 25(9): 161-164.
- [5] Pozza D, Sisto R, Durante L. Spi-Java: automatic cryptographic protocol java code generation from spicalculus[C]// proc. of the 18th Int. Conf. on Advanced Information Networking and Applications (AINA). Los Angeles: IEEE CS Press, 2004: 400-405.
- [6] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms[C]// Advances in Cryptology: Proceedings of CRYPTO 84. Berlin: Springer Verlag, 1996.

作者简介:

胡建理 男, (1976-), 博士, 工程师, 中国计算机学会会员. 研究方向为分布式计算、信息安全、数据仓库与数据挖掘和医院 MIS 系统.

李小华 男, (1954-), 博士, 主任技师. 研究方向为数据挖掘、核医学物理、医学图像处理.

周斌 男, (1971-), 副研究员. 研究方向为分布式计算、Web 服务、网络安全等.