DOI:10.13878/j.cnki.jnuist.2017.05.006

郑立新[1,2]　Jixin MA[3]　姚孝明[1]

轻量级 RFID 医疗信息系统安全协议的研究

摘要

针对未来医疗信息系统中采用轻量级射频识别(RFID)技术的安全与隐私保护问题,构建了医疗信息系统的通用流程模型,并由此提出了既有安全协议的改进方案.新方案利用业务流程中前导关联信息缩减搜索空间.安全分析表明,新方案能够有效平衡不可追踪性与伸缩性矛盾需求,抗击各类攻击,支持RFID 标签复用,且与既有 EPC C1G2 标准兼容.

关键词

射频识别(RFID);隐私保护;不可追踪性;通用流程模型;标签复用;伸缩性

中图分类号 TP309

文献标志码 A

0　引言

射频识别(RFID)技术由于能够无接触自动完成多个标签识别读取而成为物联网核心技术,在包括医疗事故预防、信息处理等领域有着广泛应用.但是,读卡器与 RFID 标签之间的信道不安全,其中交换的大量时空数据可能为恶意第三方所截获或偷听并用于数据挖掘或大数据分析,其安全性及隐私保护成为近 10 年来业界普遍关注的课题[1-3].

由于硬方法如法拉第罩等大多成本高且使用限制多,目前大多数研究人员都选择采用软方法,即通过相应的认证协议来达到期望目标.后者又大抵分为两大类:1)单个标签的双向认证协议[4];2)群组标签的双向认证协议[5-9].在上述协议方法基础上,一些方法甚至还考虑了医疗信息系统的特殊要求,如业务场地、纸质表单核查等物理限制[10-11].

RFID 技术应用的总的困难在于[12]:1)RFID 标签计算能力极其有限,难以完成复杂的密码学运算;2)标签的唯一性(unique attribute)或伸缩性(scalability)与隐私保护所需的不可追踪性(untraceability)之间的平衡.

我们发现,医疗信息系统中数据流具有显著的前导性关联流程规则特点,即除挂号模块外,其他模块都采用上一模块关联数据作为本模块的处理依据.例如,患者必须先挂号确定分诊科室,凭挂号单方可得到相关医师的诊治;住院登记也必须具备相应主治医师的意见等.这一流程规则能够为相应的匿名空间搜索提供良好的筛选机制,从而有效地解决伸缩性与不可追踪性之间的平衡问题.基于这一发现,本文首先构建了一个包括门诊和住院在内的所有业务的通用数据流程模型,围绕挂号、诊断、检查、用药等典型模块对既有协议进行评估,指出其安全漏洞,由此提出了能够弥补那些漏洞并有效解决不可追踪性与伸缩性平衡问题的改进方案,最后给出了详细的安全性分析与性能比较讨论.

1　通用数据流程模型

一般而言,患者就诊的基本流程包括:挂号、就诊、检查/检验、划价、缴费、取药、治疗、离开医院/住院等.依据文献[13],患者数据流的基本结构可概要地描述为若干子系统,如图 1 所示.

收稿日期 2017-06-25

资助项目 国家自然科学基金(61462023)

作者简介

姚孝明,男,博士,教授,研究方向为隐私保护、信息隐藏.xiaomingyao@163.com

1　海南大学　信息科学技术学院,海口,570228

2　海南大学　医院,海口,570228

3　格林威治大学　计算与信息系统系,伦敦,SE10 9LS

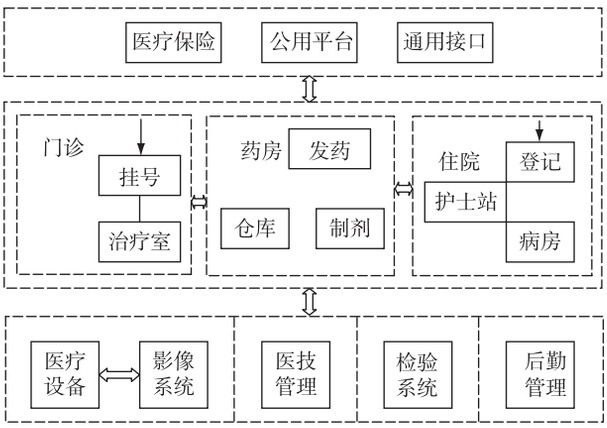

图 1　患者数据流基本结构

Fig. 1　Basic structure of the patients' data flow

图 1 中:门诊模块内的挂号以及住院模块内的登记一般都包含收费功能;各子系统模块之间的箭头反映了其中数据的共享需求及其内在的关联.更为详细的描述请参考文献[13].尽管通过业务流程再造(Business Process Re-engineering)能够改变具体模块的实际形式,但总的功能应该保持不变.尤其是,一个模块的运行常常依赖于其前导模块的前一时间的关联决策信息.换言之,若不考虑针对历史数据实施的非实时大数据分析功能,除挂号模块外,大多数子系统实时模块在某个时间段的运行都具有一份事先确定的"任务单",这份任务单所包含的信息需要与待处理的患者实时信息(纸质单)相一致.基于此,我们构建模块数据流程通用模型如下:设模块名称为通用,任务单为系统分配到该模块的任务时间序列,该序列数据按某个设定时间进行更新,患者实时信息为到场患者实际持有纸质单信息,则对应的数据流程通用模型如图 2 所示.

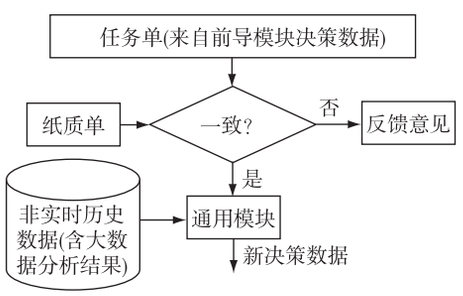

图 2 数据流程通用模型

Fig. 2　The generalized model of patients' data flow

图 2 中,若患者所持纸质单内容与系统给出的任务单信息不一致,则根据具体情况做相应的反馈处理.此外,该模型用于挂号模块时需要考虑其初始化状态,若已初始化,则可以沿用上述通用模型,否则采用初始化过程.

2　相关工作

典型的 RFID 系统一般由 RFID 标签(tag)、读卡器(reader)以及后台服务器等构成.既有协议设计假定读卡器与后台服务器之间的通信是安全的,而读卡器与标签之间的不安全信道则存在前向与后向双重安全问题,包括身份假冒、截获、信息篡改等攻击形式[3-5,10-11].囿于被动式 RFID 标签本身计算能力的局限,难以采用基于高级密码学的协议方法,而非密码学方法又无法满足相应的安全要求,近年来一些研究人员提出采用相对简单的密码学方法来实现相应协议集的设计,例如:要求标签芯片能够完成诸如单向函数、伪随机数生成器等运算,使得标签芯片门电路数量在 5 000 个左右.

文献[3]提出了包含 RFID 标签发放在内的 8 个典型场景的安全协议集,声称能够满足患者匿名、数据私密性、数据完整性、不可抵赖性,还可抵抗重放攻击,并且具有良好的系统效率.尽管其相应协议集设计相对全面,但仍然存在以下主要的安全漏洞:

1)标签发放协议:患者初始标签 PID 在读出患者所持有的智能卡内的密钥 K 后在后台服务器对 PID 采用高级加密算法 AES 进行加密得到 $x=AES(PID,K)$,将该值与系统随机分配给 PID 的假名 pseu 一起替换原 PID 存入标签.这种做法能够有一定的匿名保护作用,但是算法给出的迭代更新过程存在去同步的潜在可能,导致 DoS 攻击;此外,该算法的标签假名更新过程并非通过安全信道完成,PID 与 x 可能同时被攻击者截获,从而导致密文-明文对攻击.

2)典型场景协议:设计中考虑了后台服务器中的共享秘密对认证过程做了简化,系统效率有提高,但由于协议中认证实际上并非双向,其安全性难以保障.例如,在就诊场景中,就诊室读卡器发送一个随机数 n 给标签,后者利用该随机数 n 以及标签内部的 x 计算得到 m,并将 m,n 以及标签假名 pseu 一起发送给读卡器进行验证.由于 pseu,x 和 n 均可通过窃听得到,而 m 计算算法是公开的,因此,攻击者可以通过假读卡器获得这些信息.尤其是,pseu 以及 x 在这里实际上唯一地定义了该患者标签,从而成为该患者独有的身份标志,使得非法跟踪成为可能,导致患者隐私的泄露.

文献[4]采用希尔密码方法实现了标签身份在不安全信道的秘密传输,无需更新,因而能够有效抗击去同步攻击.但是,该方案所采用的希尔密码需要完成一系列矩阵运算,对标签的存储以及计算能力要求较高,不太适用于标签数量非常多、成本限制较高的场合.

文献[5]提出首先通过一个安全信道生成一个与 PID 绑定的密钥 K_{ts},将之与服务器生成的一个伪随机数 Trseq 一起共同作为标签的身份标识.为了应对去同步攻击,服务器事先还需要生成一组"紧急"密钥与假名数对.由于密钥 K_{ts} 仅后台服务器可见,在双向认证条件下是安全的.但是,该方案对标签密钥与假名数对的更新,仅通过来自读卡器的认证信息决定,因而易于因信息被阻断而失去同步.在去同步情况下,紧急密钥、假名数对的搜索空间则是指数级的,其系统伸缩性难以有好的表现.

文献[6-9]则提出,为了加强医院用药安全,不仅要求协议具备双向认证特性,而且还需要根据场景性质实现多标签共存认证(yoking protocol)或群组认证(grouping protocol).

目前为止,研究人员似乎普遍关注在 RFID 系统本身不安全信道的安全防护上面,尚无与医疗信息系统业务流程特点相结合的方案.其实,医疗信息系统本身即其安全防护的前提条件,是相应安全方案的重要组成部分.为此,本文依据上述通用流程模型,通过对既有协议集进行改进设计,以达到其秘密性、完整性、可用性、可审计性及不可抵赖性等安全要求,并能够有效地在系统效率以及安全保障两者之间实现平衡.

3 改进协议方案

新的改进协议方案由 3 个基本对象构成:后台服务器、读卡器以及 RFID 标签(依不同场景需同时认证的数量会有所不同).并且假定:后台服务器与读卡器之间的通信信道是安全的,读卡器与 RFID 标签之间则是不安全信道,其中读卡器与标签均可能假冒.为与医疗信息系统中药品、血液以及其他设备的追溯召回及防伪要求相一致,本方案遵守其相应的物品 RFID 标签处理,确保其符合 EPC Global[14] 网络的标准.为此,本方案所指 RFID 标签若无特殊说明均仅限于医务人员以及就诊患者所持有,与任何物品无关.

新协议方案有两个不同阶段功能目标:1)标签设置阶段:主要在挂号、缴费模块,用于对 RFID 标签进行身份绑定即状态更改处理.2)双向认证阶段:主要针对患者就诊、检查、取药等一些业务流程中加强信息安全以及用药安全等方面的身份认证处理.

3.1 标签设置

患者就诊以及医务人员入职,需要分配一个与其身份相绑定的 RFID 标签.一般而言,患者标签设置可以在挂号室完成;医务人员标签,可以在人事部门完成.这两个部门可以备有一间专用标签设置工作室,采用相应的无线通信屏蔽保护技术及专用人员管理策略,并且保存相应处理历史记录,确保该信道安全可信、可审计.设 $PRNG(x)$ 为种子 x 的伪随机数发生器函数,$H(x)$ 为将信息 x 映射为指定长度 L 的无碰撞单向函数,ID 为绑定对象的身份证信息,T_s 为服务器时间戳,⊕为异或运算,S 为状态值,则该协议过程如图 3 所示.

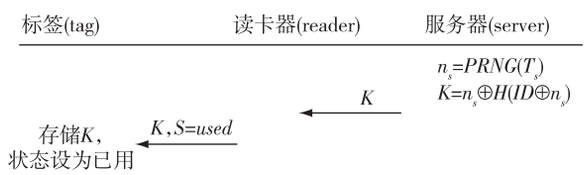

图 3 安全信道内的标签设置协议

Fig. 3 Protocol for tag setup in a secure channel

第 1 步:后台服务器通过交互界面获取相关人员的身份证信息 ID,将起始时间 T_s 作为其时间戳;以时间戳 T_s 作为种子值,采用伪随机数生成器函数得到随机值 n_s;采用无碰撞单向函数 $H(x)$ 以及异或运算⊕计算得到与相关人员身份证信息相绑定的秘密信息 K.后台数据库增加人员信息记录:ID,T_s,K.随后,服务器将秘密信息 K 发送给读卡器.

第 2 步:读卡器接收秘密信息 K,对标签发起查询,并将状态值 S 和秘密信息 K 发送给标签,S 作为 96 bit 的全 1 二进码替换原标签的 EPC 码标识已用状态,K 则存储到标签门电路输入数据存储器区域.

至此,标签已成功与相关人员身份绑定.

一旦相关人员交还标签,则需要对标签进行解绑处理.这时,仅需要通过授权人员在标签设置工作室内采用读卡器对标签发起查询,并令 $K=0$,$S=0$.标签接收到相应信息后即可完成身份解绑处理.需要强调的是,仅当发放以及收回标签时才有标签写操作,因此客观上能够严格限定其使用,例如采用硬件锁以禁止其他条件下的写操作.

3.2 双向认证

前述通用数据流程模型(图 2)表明,传统排队服务系统的输入有两个途径:1)内部数据流形成的分类任务单(AL);2)由患者或其陪同人员持有的纸质单,如挂号单、用药处方、检查申请单等.RFID 标签的采用可以实现“无纸化”,即免除纸质单的流通,但是其有效性取决于 RFID 标签认证的安全性.根据医疗业务流程用药安全性要求,将双向认证实际应用场景分为两类:1)单读卡器、单标签之间的双向认证,如患者与医生工作站的认证以确定患者就诊对应的主治医生,患者与检查室护士站的认证以确定患者检查对应的检查室与检查师等;2)单读卡器、多标签之间的双向认证,如患者到护士工作站打针、到药房取药等.

场景 1 单读卡器、单标签之间的双向认证协议

协议设计以排队服务系统为基础,其时间窗口的设置可依据医院诊疗规模的统计数据确定并动态调整,从而确保任务单内排队人数在某个固定值以内.完整协议如图 4 所示.

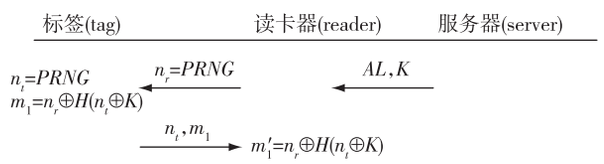

图 4 单读卡器、单标签之间的双向认证协议

Fig. 4 Mutual authentication protocol for single reader and single tag

第 1 步:服务器按照时间窗口确定各科室的实时任务单(AL),并将随同相应的秘密信息一道发送给相应科室排队服务系统指定的读卡器.

第 2 步:读卡器以本次轮询启动时间戳为种子生成一个随机数 n_r,并记录下来;将 n_r 广播给相应的标签.

第 3 步:标签门电路生成一个随机数 n_t,并进而计算 $m_1=n_r\oplus H(n_t\oplus K)$;将 n_t 与 m_1 反馈给读卡器.

第 4 步:读卡器根据 AL 以及相应的 K,本地保存的 n_r,接收到的 n_t,遍历 AL 计算 m_1';与 m_1 匹配的 K 即为相应的人员身份秘密,据此可以打开相应的任务单内内容.

由于 AL 内需要遍历的数量是个固定值,其计算复杂度为 $O(1)$.

场景 2 单读卡器、多标签之间的双向认证协议

这种场景条件下,系统需要维护 3 种对象表单:1)患者排队任务单;2)当值医务人员名单;3)药品、血液或样本表单.其中,为了减少相应医疗错误,第三种对象表单需要提供物品与相应使用者的捆绑信息 B,可以在相应部门核验完成后自动生成.例如,药房药剂师根据医师处方审核通过后即可将处方药品信息与指定患者身份信息 K 绑定.设 $F(x)$ 为该绑定过程函数,则 $B=F(K)$.

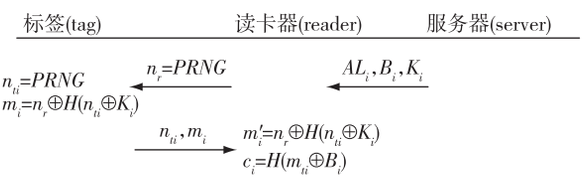

图 5 单读卡器、多标签之间的双向认证协议

Fig. 5 Mutual authentication protocol for single reader and multiple tags

第 1 步:服务器将生成的分类表单 AL_i、捆绑信息 B_i 以及秘密信息 K_i 发送给相应的读卡器.

第 2 步:读卡器以本次轮询时间戳为种子生成一个随机数 n_r,并记录下来;将 n_r 广播给相应的标签.

第 3 步:在场标签,其门电路随后生成相应随机数 n_{ti},并计算 $m_i=n_r\oplus H(n_{ti}\oplus K_i)$;将 n_{ti} 与 m_i 反馈给读卡器.

第 4 步:读卡器根据 AL_i、B_i 以及相应的 K_i,本地保存的 n_r,接收到的 n_{ti},遍历 AL_i 计算 m_i';由此确定与 m_i 匹配的 K_i,以及相应的捆绑信息 B_i.若匹配成功,则可以生成证书 $c_i=H(m_i\oplus B_i)$,否则,视群组对象不完整,将其相关信息移至下一时间窗口任务单之首等待重新匹配认证.若超过一定时间范围,群组对象仍然不完整,则系统依据 m_i'、m_i 匹配情况确定缺失对象,并给出反馈结果.根据系统内部大数据分析,甚至可以提出缺失对象的缘由可能性.

分类表单 AL_i 在相应时间窗口内均为固定值,故其计算复杂度为 $O(1)$.

4 安全性分析及性能比较

4.1 安全性分析

匿名性与信息秘密性 匿名性及信息秘密性系在读卡器与标签之间的不安全信道之间交换的数据具有不可分辨性(indistinguishability)或不可追踪性(untraceability).

证明 从上述协议方案可以看到,在不安全信道交换的信息只有两种:一是随机数;一是某种函数运算的计算结果.因此,在未知其中秘密信息的条件下,是无法反向推出函数里面的因子的.

进一步,由于不同标签生成的随机数其分布是随机的,因此,彼此之间相同与不同的几率均为50%.依据随机数对标签进行追踪得到结果与随机猜测是一致的.即使恶意攻击者获得标签内部秘密 K,由于未知相应的任务单,无法确定该标签应该对应的读卡器,从而难以通过双向认证.

更进一步可以推出,由于中间数据仅仅为本轮随机数与计算结果,且无秘密信息更新,从而不存在同步及重放问题.此外,由于任务单本身的封闭性,攻击者无法得到有效的读卡器与标签匹配关系,难以实施中间人攻击.

伸缩性(scalability) 协议算法不受整体规模影响.

证明 以上已经说明,算法复杂度均为 $O(1)$.

4.2 性能比较

从协议安全性能以及计算性能分别与既有方案相比较,结果分别如表1和表2所示.

可见,无论从安全性能或计算性能来看,本方案均优于既有方案.

表1 安全性能比较

Table 1 Comparison of security performance

	文献[7]	文献[8]	文献[9]	文献[6]	本方案
标签加密方法	PRNG	PRNG	PRNG	PRNG	PRNG
双向认证	否	否	否	是	是
匿名性	否	否	是	是	是
EPC Global C1G2 标准	不一致	一致	一致	一致	一致
伸缩性	是	是	否	是	是

表2 计算性能比较

Table 2 Comparison of computational performance

	文献[7]	文献[8]	文献[9]	文献[6]	本方案
标签	21XOR+2PRNG+9H	4XOR+6PRNG	21XOR+2ADD+23PRNG+2COMP	23XOR+4PRNG+2COMP+3SUB	1PRNG+2XOR+1H
搜索成本	$O(1)$	$O(1)$	$O(n)$	$O(1)$	$O(1)$

注:COMP 为比较,SUB 为减法,H 为单向函数,PRNG 为随机数生成器,XOR 为异或.

5 结束语

依据医疗信息系统业务流程标签发放与收回的应用特点,结合患者就诊过程中数据流的计划性,能够有效地利用系统内部安全数据构造相应的任务单.通过在标签内部事先存入秘密信息,使得在不安全信道中数据交换仅仅限于随机数以及某种计算结果,从而在具有更强安全性的基础上,获得较好的安全性与伸缩性之间的平衡.考虑到新协议方案的有效性依赖于标签写特性,下一步工作将针对标签读写硬件性质展开深入研究.

参考文献

References

[1] Rahman F,Bhuiyan M Z A,Ahamed S I.A privacy preserving framework for RFID based healthcare systems[J]. Future Generation Computer Systems, 2017, 72:339-352

[2] Sundaresan S,Doss R,Piramuthu S,et al.A secure search protocol for low cost passive RFID[J]. Computer Networks,2017,122:70-82

[3] Yeh K H,Lo N W,Wu T C,et al.Secure e-health system on passive RFID: Outpatient clinic and emergency care[J]. International Journal of Distributed Sensor Networks,2013(5):135-143

[4] Wu Z Y,Chen L,Wu J C.A reliable RFID mutual authentication scheme for healthcare environments[J].Journal of Medical System,2013,37(2):1-9

[5] Gope P,Hwang T.A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system[J]. Computers and Security, 2015, 55(C):271-280

[6] Chen C L,Wu C Y.Using RFID yoking proof protocol to enhance inpatient medication safety[J]. Journal of Medical System,2012,36(5):2849-2864

[7] Huang H H,Ku C Y.A RFID grouping proof protocol for medication safety of inpatient[J].Journal of Medical System,2009,33(6):467-474

[8] Chien H Y,Yang C C,Wu T C,et al.Two RFID-based solutions to enhance inpatient medication safety[J]. Journal of Medical System,2011,35(3):369-375

[9] Peris-Lopez P,Orfila A,Hernandez-Castro J C,et al. Flaws on RFID grouping-proofs. Guidelines for future sound protocols[J].Journal of Network & Computer Applications,2011,34(3):833-845

[10] Najera P,Lopez J,Roman R.Real time location and inpatient care systems based on passive RFID[J].Journal of Network and Computer Applications, 2011, 34(3):980-989

[11] Yen Y C,Lo N W,Wu T C.Two RFID-based solutions for secure inpatient medication administration[J].Journal of Medical System,2012,36(5):2769-2778

[12] Deursen T.50 ways to break RFID privacy[M]//Fischer-Hubner S,Duquenoy P,Hansen M,et al. Privacy and Identity Management for Life.Heidelberg:Springer,2011,352:192-205

[13] 曹雪莲.医院信息化与医院业务流程重组研究[D].武

汉:华中科技大学管理学院,2006:25-54
CAO Xuelian.Study on hospital informatization and business process reengineering[D].Wuhan:School of Management,Huazhong University of Science & Technology,2006:25-54
[14] EPC Global. EPC radio-frequency identity protocols Class-1 Generation-2 UHF RFID protocol for communications at 860MHZ-960MHZ version 1.2.0[R].2008

Security protocols for light-weight RFID-enabled healthcare information system

ZHENG Lixin[1,2] Jixin MA[3] YAO Xiaoming[1]
1 College of Information Science & Technology,Hainan University,Haikou 570228
2 Hainan University Hospital,Hainan University,Haikou 570228
3 Department of Computing and Information Systems,University of Greenwich,London SE10 9LS,UK

Abstract In order to address the security and privacy issues for future e-healthcare systems using lightweight RFID (radio frequency identification) technology,a generalized medical processing model is built,and an improved scheme on existing protocols is thus proposed.In this new scheme,information from the immediate predecessors is fully used to reduce the searching space.Security analysis shows that it can effectively tradeoff the conflicts between the security and scalability,resist all kinds of attacks,support the reuse of RFID tags,and conform to current EPC C1G2 standards.

Key words RFID (radio frequency identification); privacy protection; untraceability; generalized processing model; reuse of RFID tags; scalability