基于 Key 值更新随机 Hash 锁的 RFID 隐私保护研究

张 伟,陶志荣
ZHANG Wei,TAO Zhi-rong

江南计算技术研究所,江苏 无锡 214083
Jiangnan Institute of Computing Technology and Researching,Wuxi,Jiangsu 214083,China
E-mail:prosche_1107@hotmail.com

ZHANG Wei,TAO Zhi-rong.Research on Key Value Renewal Random Hash Lock-based RFID privacy enhancement. Computer Engineering and Applications,2008,44(32):126-128.

Abstract: On the basis of the existed way of using Key Value Renewal Random Hash Lock to enhance the security of RFID system and by the use of the minimum form of authentication protocol using challenge-response,we proposed an improved RFID authentication protocol to give more protections for the location privacy.Through this approach,the tag's response becomes random every time.Unauthorized location track will be impossible.

Key words: Radio Frequency Identification(RFID);authentication;random Hash lock;location privacy

摘 要:在当前已有基于 Hash 函数增强 RFID 安全性的方法基础上,利用基于挑战-响应方式互相认证协议最小形式,针对已有的 Key 值更新随机 Hash 锁泄漏位置隐私的安全威胁,提出了一种改进的 RFID 互相认证方法。该方法弥补了已有研究的不足,对标签的响应增加了随机性,可以更好地应对位置隐私泄漏的威胁。

关键词:射频识别;认证协议;随机 Hash 锁;位置隐私
DOI:10.3778/j.issn.1002-8331.2008.32.037 **文章编号:**1002-8331(2008)32-0126-03 **文献标识码:**A **中图分类号:**TP309.1

1 引言

射频识别(Radio Frequency Identification,RFID)技术,是一种利用射频通信实现的非接触式自动识别技术。RFID 标签具有体积小、容量大、寿命长、可重复使用等特点,可支持快速读写、非可视识别、移动识别、多目标识别、定位及长期跟踪管理[1]。但由于未授权的读写器可以读取和收集其作用范围内电子标签的相关信息,并通过信息积聚或与位置信息对照来获取消费者的隐私信息,加之无线通信本身固有的脆弱性,因而 RFID 系统的安全引起了人们的极大关注。

2 RFID 系统组成及其安全挑战

2.1 系统组成概述

一套完整的 RFID 系统,如图 1 所示,由读写器(Reader)与电子标签(Tag)也就是所谓的应答器(Transponder)及应用软件系统三个部分所组成,其工作原理是 Reader 发射特定频率的无线电波能量给 Tag, 用以驱动 Tag 电路将内部的数据送出,此时 Reader 便依序接收解读数据,送给应用程序做相应的处理。由 AutoID 实验室提出的 RFID 标签分类[2],一般认为类别 1 和类别 2 是最低成本的标签。类别 1 拥有一个只读的存储快,而类别 2 有一些可读写的存储块。类别 1 包括的逻辑门大约为 1 000 到 4 000 个左右,而类别 2 也在 1 万以内。尽管用于认证和识别用途的密码技术已相对比较成熟,但是,到目前为止,由于组成 RFID 系统的必备设备 Tag 的特殊性和局限性, 设计安全、高效、低成本的 RFID 安全机制仍然是一个具有挑战性的课题。

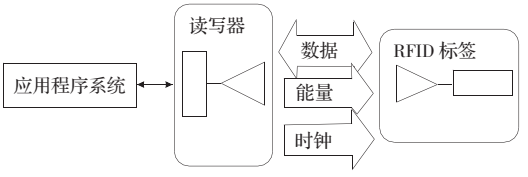

图 1 RFID 系统结构

2.2 面临的安全及隐私威胁

RFID 技术属于非接触式自动识别技术,其面临的安全隐私威胁主要有:

(1)非法读取:商业竞争者可通过未授权的读写器快速读取超市的商品标签数据,获取重要的商业信息。

(2)位置隐私:位置隐私含有高度的个人特征,携带 RFID 标签的任何人都可能在公共场合被自动跟踪,尽管多数人并不关心自己是否在公共场合被跟踪,但是像艾滋病人、宗教信徒等个人或是组织机构都要防止被自动跟踪。

(3)窃听:因 RFID 系统在前向信道的信号传输距离较远,

作者简介:张伟(1983-),男,硕士研究生,主要研究方向:智能信息处理,信息安全;陶志荣(1969-),女,高级工程师,硕士生导师,主要研究方向:网络信息处理。

收稿日期:2007-12-11 **修回日期:**2008-03-25

窃听者可轻易窃取读写器发出的信号数据,使得个人或是组织的信息隐私泄露。个人隐私包括个人信息比如纳税、医疗或者购买记录、个人习惯等;组织隐私可能包括门禁系统的认证等。

(4)非授权的标签不可用:攻击者使得标签进入不能正常工作的状态,也称为拒绝服务攻击(DoS)。结果是,标签变得暂时或是永久失效。这样的攻击常常由于标签的移动天性而变得越发严重,使得标签易于受到远处隐蔽读取器的操纵。如果不能抵抗这样的攻击,那么使用 RFID 的商店就会遭到失窃,除非使用摄像监视。

(5)伪装哄骗:通过伪装成合法标签,哄骗读写器为其提供错误的数据。这还包括非授权的标签复制,一种完整性攻击,攻击者成功地截获到标签的辨认信息后就能实现。同样,由于标签能够被欺诈的读取器所读取而使得问题更严重。能够复制标签将使得防伪保护失效,接着就能实施偷窃。而对于使用 RFID 标签进行自动化安全验证的公司,这将是一个新的易受到攻击的弱点。

(6)重放攻击:这也是一种完整性攻击,攻击者使用伪造的读取器,模拟事先截获的目标标签应答,由此模拟需要的一个标签。对于使用非接触式身份认证卡的 RFID 系统环境,这提供了一种非法进入受保护区域的手段。

(7)所列出的这些安全和隐私威胁并不能涵盖所有的攻击类型,随着 RFID 应用的深入,还将产生数不胜数的新的攻击方式,RFID 系统的安全问题不容忽视。

3　研究现状

随着 RFID 标签的推广和使用,出现了大量关于标签使用所引发安全威胁的研究。通过物理手段,例如"Kill 命令机制"[3],在售出商品时毁坏或是移除标签,缺点是无法重用且无法有效验证是否真正对 Tag 实施了 Kill 操作;标签屏蔽[4],通过一个屏蔽装置,使得标签无法接收到外界的电磁波,阻止非授权的读写器对标签的访问。缺点就是额外的屏蔽装置将带来不便和增加投入。

更多的实现是通过设计安全协议来抵抗安全和隐私威胁。文献[5]中有详细且周期更新的在线论文目录。Hash 锁机制[7],所谓的"锁",指的是一个 hash 计算的结果 hash(key),其中的 key 是一个随机值。这个"锁"值被发给标签并存储到标签的一个保留区域,标签自动进入加锁状态。如果要解锁标签,读写器需要发送原始 key 值到标签,标签将进行 hash 计算,若与其存储的值匹配就进入解锁状态,返回标签的识别号 EPC 码。此方法简单且直接保护数据,只有授权的读写器可以解锁标签并获取数据,且在获得 EPC 码后加锁标签;随机 Hash 锁机制[6],此方法是基于伪随机函数(PRFs)对 Hash 锁机制的延伸,需要在标签中额外增加一个伪随机数生成器(PRNG)。标签用一对值回应读写器的询问:$(r,\text{hash}(ID_k \parallel r))$,$r$ 是由标签产生的一个随机数,ID_k 是第 k 个标签的 ID,$\parallel$ 是连接符,读写器收到响应后,将遍历 N 个当前的 ID 值,计算数值对,如果找到匹配则发送 ID_k 解锁标签,但如果敌手获得某标签的响应$(r,\text{hash}(ID_k \parallel r))$,且将此响应发送到合法的读写器,将得到标签的 ID,且如果标签被破解则其历史位置信息也将泄漏。随机 Hash 链机制,Ohkubo 在文献[7-8]中建议使用一种链状的 Hash 过程来加强安全,每次激活标签,就计算一个新的 metaID。使用两个不同的 Hash 函数,对当前的 metaID 做一次 Hash 运算,结果作为第二个 Hash 函数的种子,将最终运算结果发送给读写器,通过遍历获取匹配于收到的值,完成验证。优点是对于重复获取 metaID 的攻击不敏感,但是每次不成功的询问所得返回都是一样的,将无法保证位置隐私。

曾丽华在文献[9]中对随机 Hash 链机制进行了扩展,提出了一种新的方法——Key 值更新随机 Hash 锁。该方法使用单向 Hash 函数添加随机 Hash 锁,并在每次通信过程中更新标签 Key 值,且标签与读写器之间的数据传输都经过了 Hash 加密,有效地防止了非法读取、窃听、伪装哄骗、重放等攻击。其基本工作原理如图 2 所示:

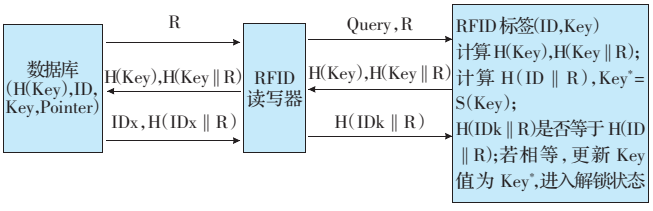

图 2　基本工作原理图

锁定标签:读写器将一个随机选取的值作为标签的 Key 值发给标签,并在数据库中建立初始记录$(H(Key),ID,Key,0)$,标签将接收到的 Key 值存储,进入锁定状态。

解锁标签:数据库产生随机数 R,由读写器发送$(Query,R)$到标签,标签根据 Key 值计算 $H(Key)$,$H(Key \parallel R)$数据对返回给读写器,并计算 $H(ID \parallel R)$和 $Key^*=S(Key)$。读写器查找数据库中的记录,若某个 $H(Key_i)$与 $H(Key)$相匹配,则计算 $H(Key_i \parallel R)$与 $H(Key \parallel R)$比较,相等认为标签合法,反之则忽略此消息。数据库根据查询记录计算 $H(Key_k \parallel R)$,并添加新的记录 j:$(H(Key_i^*),ID_k,Key_i^*,i)$,将记录 i 修改为$(H(Key_i),ID_k,Key_i,j)$,若 *Pointer* i!=0,则找到 *Pointer* i 记录,将其修改为$(H(Key_i^*),ID_k,Key_i^*,i)$。标签将收到的 $H(ID_k \parallel R)$与之前计算的 $H(ID \parallel R)$相比较,若相同,更新 Key 值为 Key^* 则标签进入解锁状态。反之则验证失败,标签保持沉默。

通过每次成功验证就更新标签及数据库中的 Key 值,使得无法获取标签相关的历史活动信息。但是该方法也有一定的缺陷:如果某段时间内,某个标签中存储的 Key 值,因为某种原因而未能更新,则此时敌手发出一个询问$(Query,R)$,该标签将返回同样的应答 $H(Key)$,$H(Key \parallel R)$。由此,可以获取标签的位置信息。即:使用此方法进行验证的标签在两次 Key 值更新之间,将无法保证位置隐私。

4　对 Key 值更新随机 Hash 锁的改进

4.1　背景知识介绍

来学嘉在文献[10]中,基于挑战-响应方式的互相认证协议,安全需求被明确表示为 7 个简单的必要条件,每一个条件和一种攻击相关联,不完全实现这些条件的协议将会遭到某种攻击,并给出了两个协议,使得它们包含所需最少的安全参数。7 个必要条件是:$R1$ 是 B 到 A 的验证;$R1$ 是对 $C1$ 的响应;$R1$ 依赖于验证过程的初始化;$R2$ 是 A 到 B 的验证;$R2$ 是对 $C2$ 的响应;$R2$ 依赖于验证过程的初始化;$R2$ 与 $C1$ 在同一个信息中。文中结论认为,这 7 个必要条件对于安全协议也是充分的。

其中的最小形式如图3所示,$C1$是Alice到Bob的随机挑战,而$C2$是Bob到Alice的随机挑战。本文将要给出的改进中,提出的认证协议就是来源于文献[10]中的最小形式。

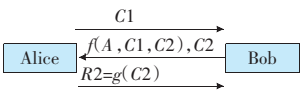

图3 认证协议的最小形式

实际实现中,需要通过有效的硬件来实现伪随机数生成器。Krawczyk在文献[11]中,使用少于2 000个逻辑门提供了约80 bit的安全性[12],这样的安全性,对于大多数的RFID应用都是可行的。

4.2 改进方法介绍

在数据库中每个标签存储两个数对,一个(ID,K_i)数对,相应存储一个指针*Pointer i*,指向上一个用过的(ID,K_j)数对,保证两个数对中一个与标签中存储的Key值相同。若标签第一次使用,*Pointer i*存储值为零。标签初始化时,由读写器写入一个初始Key值K_0,标签进入锁定状态。解锁标签需要读写器与标签通信三次,如图4所示:

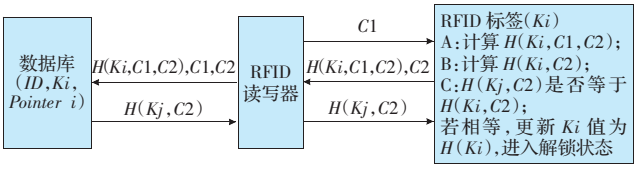

图4 解锁标签

(1)如果要解锁标签,由读写器发送一个随机生成固定长度的伪随机数$C1$到标签。

(2)标签计算$H(K_i,C1,C2)$返回给读写器,并预先计算$H(K_i,C2)$。

(3)读写器收到标签的响应后,通过安全信道发送$H(K_i,C1,C2)$、$C1$、$C2$到后台的数据库,根据记录Key值,计算$H(K,C1,C2)$,查找与收到值相匹配的记录K_j(如果没有记录相匹配,则忽略此次验证)。若有记录匹配,则使用K_j计算$H(K_j,C2)$发送到读写器并转发到标签。

(4)标签收到$H(K_j,C2)$后与之前计算的$H(K_i,C2)$比较,若相同则验证成功,读写器合法。反之,忽略此次验证。

(5)若数据库查找到匹配的K_j,则计算$H(K_j)$替代记录中指针所指向的上一次用过的Key值,并将那条记录中的指针指向当前(ID,K_j)数对。同时,若标签验证读写器合法则更新K_i为$H(K_i)$。

4.3 安全分析

本文提出的方法,由于对消息进行了Hash运算,可以抵抗对通信过程的窃听;缺少数据库支持的读写器将无法通过标签的验证,不能解锁标签,保证标签不被非法访问;由于在验证过程中使用了伪随机数,可以抵抗重放攻击,任何历史消息将被忽略,即:认证过程被打断将无法实现互相认证;同时,如果标签未收到读写器的响应$H(K_i,C2)$,则认为验证未通过,不会更新Key值,仍然保持锁定状态,阻止非法访问。最重要的是以下两点:

(1)满足7个必要条件

通过分析上文提出的方法,可知其满足文献[10]中的7个必要条件。①$R1$是标签到读写器的验证;②$R1$是对读写器发送$C1$的响应;③$R1$依赖于验证过程的初始化,即$C1$消息;④$R2$是读写器到标签的验证;⑤$R2$是对标签发送$C2$的响应;⑥和⑦$R2$依赖于验证过程的初始化是通过间接的方式,即:如果读写器无法确认$R1$的合法性,则不会发送响应$R2$。

(2)保护位置隐私

标签对读写器的响应为$H(K_i,C1,C2)$,此消息中包含K_i、$C1$、$C2$。既依赖于读写器发送的伪随机数$C1$,又依赖于标签所产生的伪随机数$C2$,由于Hash函数的单向性,无法得到运算前的值。因此,无法从标签的响应来区分,得不到标签的位置信息,弥补了文献[9]中方法的不足。相对于文献[9]中的方法,伪随机数仅来自于读写器,使得随机性在缺少合法读写器的条件下就会失去,而本文的方法,标签的响应中包含了双方产生的伪随机数,不会失去随机性。

5 结论

随着RFID广泛使用,其带来的安全和隐私问题也越发突出。出现了大量加强安全和隐私的方法,本文在综合前人工作的基础上,重点针对Key值更新随机hash锁提出了一种改进方法,通过在标签中增加一个伪随机数生成器,实现了对位置隐私更好的保护,并带来更高的安全性,适合于对位置隐私有要求的RFID应用,诸如:某些特殊人群比较关心在公共场合是否被自动跟踪,该方法能够满足基本的安全需求。但本文提出的方法中,如果读写器与标签通信正常,且标签完好,未遭到物理毁坏,就能够抵抗拒绝服务攻击。缺点是验证标签需要在数据库中搜索,不适合标签数目较多的情况。

参考文献:

[1] 中华人民共和国科学技术部等十五部委.中国射频识别(RFID)技术政策白皮书[R].2006-06-09.

[2] AutoID Labs homepage[EB/OL].http://www.autoidlabs.org.

[3] Sarma S,Weis S,Engels D.White paper:RFID systems,security and privacy implications,MIT-AUTOID-WH-014[R].Auto-ID Center,MIT,November 2002.

[4] Juels A,Rivest R L,Szydlo M.The blocker tag:Selective blocking of RFID tags for consumer privacy[C]//ACM Conference on Computer and Communications Security,2003:103-111.

[5] Avoine G.Security and privacy in RFID systems[EB/OL].http://lasecwww.epfl.ch/~gavoine/rfid/.

[6] Weis S,Sarma S,Rivest R,et al.Security and privacy aspects of low-cost Radio Frequency Identification systems[C]//1st Intern Conference on Security in Pervasive Computing(SPC),2003.

[7] Ohkubo M,Suzuki K,Kinoshita S.Hash-chain based forward-secure privacy protection scheme for low-cost RFI[C]//Proceedings of the SCIS 2004,2004:719-724.

[8] Ohkubo M,Suzuki K,Kinoshita S.Cryptographic approach to privacy-friendly tags[C]//RFID Privacy Workshop,Massachusetts Institute of Technology,Cambridge,MA,USA.

[9] 曾丽华,熊璋,张挺.Key值更新随机Hash锁对RFID安全隐私的加强[J].计算机工程,2007,33(2):151-153.

[10] LAI Xue-Jia.Security requirements on authentication protocols using challenge-response[J].中国科学院研究生院学报,2002,19(6):246-252.

[11] Coppersmith D,Krawczyk H,Mansour Y.The shrinking generator[C]//Proc Advances in Cryptology,CRYPTO 1993,1994:22-39.

[12] Batina L,Lano J,Mentens N,et al.Energy,performance,area versus security trade-offs for stream ciphers[C]//The State of the Art of Stream Ciphers,Workshop Record,2004.