RFID 系统中安全和隐私问题的研究*

王连强[1,2]，吕述望[2]，韩小西[3]

(1. 南开大学 信息技术科学学院，天津 300071；2. 中国科学院 研究生院 信息安全国家重点实验室，北京 100080；3. 中国科学院 软件研究所 计算机科学实验室，北京 100080)

摘　要：射频识别(RFID)技术的应用将给零售、物流等产业带来革命性的变化，但同时出现的安全和隐私问题却极大地限制了其使用的范围，如何在 RFID 系统中保证安全、维护个人隐私成为业界讨论的热点问题。在分析四种常见解决方案的基础上，阐明了各自的优缺点，探讨了在 RFID 系统中解决安全和隐私问题所面临的挑战，并指出了其发展的方向。

关键词：射频识别标签；安全；隐私；树型查询

中图法分类号：TP309　　**文献标识码**：A　　**文章编号**：1001-3695(2006)06-0016-03

Study of Security and Privacy Aspects in RFID System

WANG Lian-qiang[1,2]，LV Shu-wang[2]，HAN Xiao-xi[3]

(1. *College of Information Technical Science, Nankai University, Tianjin* 300071, *China*; 2. *State Key Laboratory of Information Security, School of Groduate, Chinese Academy of Sciences, Beijing* 100080, *China*; 3. *Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing* 100080, *China*)

Abstract: The application of Radio-Frequency Identification (RFID) technology will bring about revolutionary change for retail, logistics and other industry, while the application scope of RFID is restricted greatly by security and privacy aspects appeared simultaneously. Currently security and privacy aspects in RFID system are being studied aggressively. This paper analyzes four kinds of solutions, sets forth relative merits of each method. The challenges of solving security and privacy aspects in RFID system are discussed, and directions of development are presented.

Key words: RFID Tags; Security; Privacy; Tree-walking

自动识别(Auto-ID)技术在访问控制和安全应用等领域获得了广泛的应用，尤其是 20 世纪 70 年代出现的条形码技术，极大促进了供应链管理等产业的发展。最近，另外一种自动识别技术——射频识别(RFID)技术，已经在制造、零售、物流等领域显示出强大的实用价值，专家预言，RFID 技术的应用将给零售、物流等产业带来革命性的变化。

目前全世界每天要扫描的条形码数量超过了 50 亿，而且大多数仅在顾客购买商品时被扫描，RFID 技术不仅能应用于自动付账业务，而且它可为大量的应用提供服务，如产品的生产、零售、使用，甚至政府机构对产品的检查等过程。RFID 的潜在应用范围非常广泛，使用 RFID 技术的仓库管理系统将通过自动实时存货监控、自动质量控制和自动付账等流程彻底改变供应链管理过程[2]。在 RFID 技术广泛应用的同时，也出现了很多问题，它超出了原有计算机信息系统的安全边界，因此引入了新的安全和隐私风险。本文将分析 RFID 系统中存在的威胁和风险，研究目前 RFID 系统中安全和隐私保护的各种方法，阐明各自的优缺点，并指出所面临的挑战和发展的方向。

1　RFID 系统

RFID 系统包含三个主要组成部分，如图 1 所示。

收稿日期：2005-08-11；修返日期：2005-09-23

基金项目：国家自然科学基金资助项目(60277027)；国家“973”计划资助项目(TG1999035808)

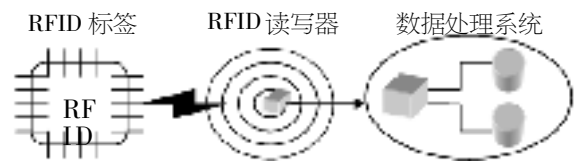

图 1　RFID 系统

(1) RFID 标签，可存储被识别对象的相关数据。RFID 标签包括一个微芯片和一个耦合元素(天线)，可通过射频进行通信，它分为主动型和被动型两种。主动型标签本身需具备能源，可主动发送 RF 信号；而被动型标签只能从读写器发出的询问信号中获得用于通信所需的能量。RFID 读写器包括射频模块、控制单元和一个耦合元素，它通过射频通信给标签发送询问信号，对标签数据进行读/写操作，数据处理系统利用读取的数据进行相关操作，如可将其作为一个产品信息数据库的查询密钥或作为跟踪日志等。

(2) RFID 读写器，能发出“询问”信号，识别相关对象，可对对象的标签数据进行读/写操作。RFID 读写器通过查询对象标签的 ID(存放于标签内)识别一个特定的对象。如果存在多个被识别的对象，读写器会收到多个响应，这些响应将互相影响，从而发生冲突。因此 RFID 系统需要一个防冲突算法，目前主要的解决方案包括概率型算法和确定型算法两种。

Aloha 机制是大家比较熟悉的概率型算法[3]，可用于以太局域网。它规定 RFID 标签以一个随机的时间间隔响应 RFID 读写器的询问，从而尽可能避免冲突。当发生冲突时，RFID 标签将等待随机的时间间隔，然后重试。在这种机制中，如果要

读取的标签过多, 将导致高冲突率, 从而降低标签的查询效率。

确定型算法的一个例子是二进制树型查询算法。在此机制中, 假设标签的 ID 为 k 位, 所有可能的 ID 将被视为一个深度为 k 的标准二进制树的叶, 树中除叶之外的所有节点都有两个枝: 左枝和右枝, 分别表示 "0" 和 "1"。树根的深度为 0, 且为空串, 深度为 d 的节点代表二进制串 $B = b_1 b_2 \cdots b_d$, 表示从根到此节点所经过的所有枝的序列集合。如果 $d < k$, 此节点有两个枝, 对应两个子节点, 深度皆为 $d+1$, 左边子节点的串为 $x \| 0$ (意指 x 串联 0), 右边子节点的串为 $x \| 1$; 如果 $d = k$, 则此节点为二进制树的叶, x 长度为 k, 对应于相应的 ID。

(3) 数据处理系统, 利用从 RFID 读写器获得的标签数据进行相关操作。

树型查询过程实际上是由读写器执行的一个递归的深度搜索过程。设一个节点的子树表示树中此节点的所有后代, 给定一个节点 $B = b_1 b_2 \cdots b_d$, 读写器将查询 B 的子树中所有具有前缀 $b_1 b_2 \cdots b_d$ 的标签, 其他标签则处于静止状态。被查询的标签将其 $d+1$ 位传给读写器, 例如, 如果标签位于节点 B 的左边子树, 它将传送 "0"; 位于右边子树则传送 "1"; 如果既有位于左边子树的标签, 也有位于右边子树的标签, 将同时返回 "0" 和 "1", 从而导致冲突。在这种情况下, 读写器将按顺序从子节点 $B \| 0$ 和 $B \| 1$ 开始递归查询。如果标签都返回位 b (0/1), 表示标签位于相同的子树中, 读写器将从节点 $B \| b$ 开始递归查询。当查询过程到达树的一个叶时, 它将输出相关的 k 位序列码, 即所识别的标签 ID, 此算法的所有输出是可读范围内的所有标签 ID 的列表。

2　安全和隐私风险

为实现信息安全, 很多组织已经进行了大量投资, 建立了诸如防火墙、入侵检测、VPN、PKI/CA 等设施, 这些措施在一定程度上可以解决组织内部存在的安全问题。但由于 RFID 系统的数据源和访问界面扩大了安全周边的范围, 因此引入了原有控制措施无法有效解决的新风险。

按照人们的设想, RFID 标签 ID 不仅要包含传统条形码所包含的内容, 而且它将是标签唯一的序列码, 通过它将唯一地识别对象。但标签可以响应任何 RFID 读写器的询问信号, 所有拥有读写器的人员或机构都可访问缺乏访问控制的标签, 安全问题显而易见。

一个 RFID 读写器能够识别带有 RFID 标签的对象位置, 从位于多个地点的读写器中收集相关的数据便可以追踪对象的移动路线, 即使对标签采取了保护措施, 他们仍然可以通过检测标签的异常响应信号而跟踪对象的移动。更为严重的是, RFID 读写器的传输信号能在几公里之外通过射频扫描器和天线获得, 如果此传输信号没有被保护, 将会导致数据的未授权访问, 标签 ID 被假冒、复制或重放, 从而危害 RFID 系统的安全。另外, RFID 系统中存在标签欺骗问题, 如一个超市内的 RFID 系统, 偷盗者可通过标签欺骗, 使自动检验设备误认为被拿走的物品还在原处, 或者利用其他物品的标签 ID 替代高价值物品的标签 ID, 从而达到自己的目的。

针对上述安全问题, 已经出现多种解决方法, 但大多只是针对某一安全问题而提出的, 还没有一种方法能够完全满足所有的安全需求。

3　RFID 系统安全解决方法分类

3.1　摘要锁方法

摘要锁方法中 RFID 标签可以被 "锁定"。在锁定状态下, 标签对 RFID 读写器发出的除解锁信号之外的所有询问信号都将返回解锁密钥的摘要值, 而不是标签的 ID, 此方法基于单向摘要函数[1]。

锁定一个标签时, 标签所有者要在标签中存储一个随机密钥 Key 的摘要值作为标签的 Meta-ID, Meta-ID = hash(Key), 其中 hash 为单向摘要函数, Key 可以是个人识别码或口令, 系统将 Key 和 Meta-ID 一起存放于数据处理系统的后端数据库中。标签在收到 Meta-ID 后, 将自身设为锁定状态。

要解锁一个标签, 合法读写器询问标签的 Meta-ID, 并从后端数据库中搜索对应的 Key 作为解锁信号传送给标签, 标签将对 Key 做摘要运算, 并与其 Meta-ID 比较, 如果一致, 解除锁定状态并返回其 ID。在实际应用中为防止对未锁定标签的攻击, 标签解锁后一般只执行一次响应, 然后重新锁定。

基于单向摘要函数的逆向运算困难, 此方法可防止未授权用户利用 Meta-ID 计算 Key 值, 从而达到防止标签 ID 泄漏的目的。但摘要锁方法的一个缺点是无法抵抗 "中间人攻击", 一个攻击者可以询问标签的 Meta-ID, 然后以重放攻击方式将其发给合法读写器, 读写器按照规定的流程将返回对应的 Key 值, 攻击者便可利用 Key 值得到标签的 ID。

3.2　重加密方法

为防止伪造并方便政府机构对犯罪交易进行追踪, 欧洲中央银行提出 2005 年要在其大面额纸币中嵌入 RFID 标签。但要实现此目标, RFID 系统的安全问题首先必须得到解决, 重加密方法就是针对此安全问题而提出的一种解决方法[4]。为增强安全性, 重加密方法使用目前流行的公钥加密机制。公钥加密机制运算量大、资源需求较多, 由于受成本影响, RFID 标签的运算资源受到严格限制, 所以重加密方法将密码运算交由外部代理完成, 标签本身不执行运算, 只存储相关数据。

本方法中, 假设 CS = (KG, Enc, Dec) 表示公钥加密机制, 其中 KG 表示密钥产生函数, Enc 和 Dec 分别表示加解密函数。设 DS = (SKG, Sig, Ver) 表示公钥数字签名机制, 其中 SKG 表示密钥生成函数, Sig 和 Ver 分别表示签名和验证函数。此机制的合法参与方包括用户、银行 B、商人 M 和政府机构 L。

初始化时银行 B 产生一个数字签名密钥对 (PK_B, SK_B), 同时政府机构 L 产生一个加密密钥对 (PK_L, SK_L), 公钥 PK_B 和 PK_L 公开, 另外此方法还需要一个公开的单向摘要函数 h。对纸币 i, B 选择一个唯一的序列码 S_i, 并计算签名 $U_i = Sig(SK_B, [S_i \| den_i])$, 这里 den_i 表示纸币的币值, 将其放入签名中可防止币值替换的假冒攻击, 币值的标识符也可以包括在 S_i 中。另外, B 还要产生纸币的访问密钥 $D_i = h(U_i)$。B 将以可视解码的方式将 S_i 和 U_i 印在纸币上, 可视解码机制要便于商人使用机器自动进行识别, 如条形码机制。然后 B 将使用 L 的公钥加密 S_i, U_i 和随机产生的加密因子 r_i, 密文 $C_i = Enc(PK_L, [U_i \| S_i], r_i)$, 将 C_i 存入标签的内存单元 M1 中, 将 r_i 存入标签的内存单元 M2 中, 同时记录纸币的序列码和币值。

图 2 提供了本方法中标签存储内容的图示(无下标)。

	单元 M1:密文	单元 M2:加密因子
RF	$C = Enc(PK_L, [U \| S], r)$	r
	写密钥为 $D = h(U)$	读/写密钥都为 $D = h(U)$
	序列码	签名
可视	S	$U = Sig(SK_B, [S \| den])$

图 2 标签数据图

商人 M 在商品交易中收到用户的纸币时,首先要验证纸币的正确性,过程如下:①以可视化机制读取 S_j 和 U_j;②计算 $D_j = h(U_j)$;③从 M1 中读取 C_j,并利用 D_j 从 M2 中读取 r_j,如果读取 r_j 失败,将纸币上交政府机构;④检查 C_j 的值是否等于 $Enc(PK_L, [U_j \| S_j], r_j)$,如果不相等,无效密文要提交政府机构;在验证纸币的真伪后,M 替换原密文 C_j,即重新加密过程;⑤M 随机产生 r_j',并利用 D_j 将其写入 M2,如果写入失败,将纸币上交政府机构;⑥计算新密文 $C_j' = Enc(PK_L, [U_j \| S_j], r_j')$,并利用 D_j 将其写入 M1,如果有错误发生,报告政府机构。

政府机构对纸币的跟踪过程如下:①L 读取目标纸币 RFID 标签中 M1 的内容获得密文 C;②利用 SK_L 解密 C,得到 U 和 S;③L 将检查 U 是否是 S 的一个有效签名,如果是,说明纸币为真,L 获得序列码 S。

重加密方法的安全性依赖于公钥加密机制和摘要函数,安全性较高,但未有效解决用户隐私问题。此方法所需资源也比较多,虽然 RFID 标签无须执行密码运算,但加密代理设备、可视化机制验证设备等成本较大,另外,此机制还需要标签至少具备几百位的存储空间,这将增大标签的成本。因此重加密方法不适用于为普通低价值物品所设计的系统。

3.3 阻塞标签方法

阻塞标签方法基于上面介绍的二进制树型查询算法,使用"阻塞标签"来达到保护用户隐私的目的[5]。阻塞标签通过模拟标签 ID 的方式干扰算法的查询过程。

阻塞标签可模拟 RFID 标签 ID 的所有可能的集合,从而避免标签的 ID 被查询到。当 RFID 读写器为确定 ID 的某位而询问一个节点 *B* 的枝时,阻塞标签将同时广播"0"和"1",这种强制性冲突使读写器在该节点发生递归;同样在下一节点读写器仍将同时收到"0"和"1",这将导致读写器遍历整棵树。如果有足够的内存、处理能力和处理时间,RFID 读写器将输出所有可能的 ID。

也可将阻塞标签模拟 ID 的范围定为二进制树的某子树,子树内的标签有固定的前缀,当读写器查询 ID 的固定前缀时,阻塞标签不发生作用;但查询前缀后的位时,阻塞标签将阻碍查询过程,如一个选择性阻塞标签只在查询树根左边的枝时才响应,这将导致读写器在查询以"0"为前缀的 ID 时受到阻碍,而查询以"1"开头的 ID 时不受影响。通过这种方式,选择性标签能保护一个特定域。实际上,一个选择性阻塞标签可以用于阻止读写器查询具有任意固定前缀的标签。

当阻塞标签阻塞特定域(子树)时,将影响其他正常区域标签的查询,如在查询以"0"开头的 ID 时被阻塞,读写器可能永远不能查询以"1"开头的 ID。因此需要一种方法使 RFID 读写器不查询被阻塞的子树,即读写器需要知道哪一个子树被阻塞,以便它查询树的其他部分。其中一种解决方案是修改树型查询算法:读写器在查询树中某节点的枝前,先询问此节点的子树是否被阻塞,标签将返回结果,如果没有被阻塞,读写器按原流程继续处理;如果被阻塞,则读写器查询其他部分。

阻塞标签方法的优点是 RFID 标签基本不需要修改,也不必执行密码运算,减少了投入成本,并且阻塞标签本身非常便宜,与普通标签价格相差不大,这使得阻塞标签可作为一种有效的隐私保护工具。但同时阻塞标签也可能被用于进行恶意行为:通过模拟标签 ID,恶意阻塞标签能超出规定 ID 隐私保护的范围,从而干扰正常的 RFID 应用。RFID 读写器能够处理隐私区域内的阻塞行为,但它的主要功能是查询此区域外的标签,因此恶意阻塞标签能对系统进行拒绝服务攻击,破坏 RFID 系统的正常服务。

4 结束语

RFID 技术已经在零售、物流等领域内展示出其强大的优越性,在未来的发展中必将给我们日常生活带来极大的便利,但安全和隐私问题不容忽视。从前面的论述中可以看出,研究人员提出了许多方法解决 RFID 系统的安全和隐私问题,也取得了一定效果,但这些方法都有各自的优缺点,不能完全满足 RFID 系统的安全需求,达到真正实用的目标。这也说明解决 RFID 系统的安全和隐私问题是一件困难的事情,原因主要在于要大规模推广使用 RFID 技术,必须严格限制标签的成本,而低成本的标签又极大限制了其安全和隐私问题的解决。

通过分析,有效解决 RFID 系统的安全和隐私问题将取决于以下三个方面的发展:①最关键的研究领域仍然是开发和实施硬件实现的低成本的密码函数,包括摘要函数、随机数发生器以及对称加密和公钥加密函数等;②在电路设计和生产上进一步降低 RFID 标签的成本并为解决安全问题分配更多的资源;③设计开发新的更有效的防偷听、错误归纳、电力分析等的 RFID 协议。一般而言,RFID 读写器和标签必须能在不影响安全的情况下从能源或通信中断中平稳恢复。

综合考虑上述三个方面,研究有效的解决方案将是未来 RFID 技术发展的主要方向。

参考文献:

[1] A Weis, S Sarma, R Rivest, *et al*. Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems[C]. The 1st International Conference on Security in Pervasive Computing, volume 2802 of Lecture Notes in Computer Science, 2004. 201-212.

[2] Sanjay E Sarma, *et al*. RFID Systems and Security and Privacy Implications[C]. Workshop on Cryptographic Hardware and Embedded Systems, Lecture Notes in Computer Science, 2002. 454-470.

[3] Robert M Metcalfe, David R Boggs. Ethernet: Distributed Packet Switching for Local Computer Networks[J]. Communications of the ACM, 1976, 19(5): 395-404.

[4] A Juels, R Pappu. Squealing Euros: Privacy Protection in RFID-enabled Banknotes[C]. Financial Cryptography '03, 2003. 134-145.

[5] A Juels, R Rivest, M Szydlol. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy[C]. The 8th ACM Conference on Computer and Communications Security, ACM Press, 2003. 103-111.

作者简介:

王连强(1977-),男,博士研究生,主要研究方向为信息安全、网络安全;吕述望(1941-),男,研究员,博士生导师,主要研究方向为密码学、信息安全;韩小西,博士研究生,研究方向为密码学。