第35卷 第15期 计 算 机 工 程 2009年8月
Vol.35 No.15 Computer Engineering August 2009
·安全技术· 文章编号：1000—3428(2009)15—0143—03 文献标识码：A 中图分类号：TP309

RFID标签所有权转换模式及协议设计

邵 婧[1]，陈 越[1]，常振华[2]
（1. 解放军信息工程大学电子技术学院，郑州 450004；2. 解放军69031部队，乌鲁木齐 830000）

摘 要：针对射频识别标签所有权转换过程的安全隐私问题，提出一种“先授权后更新”的所有权转换模式，并设计相应的实现协议。在密钥协商后，把标签的全部相关信息安全地转交给新的所有者。在相互认证的基础上，安全更新标签秘密，使得原所有者无法再对标签进行查询。该方案保证所有权转换过程中新用户的隐私安全。

关键词：射频识别；所有权转换；授权；密钥协商；安全

Design of RFID Tag Ownership Transfer Mode and Protocols

SHAO Jing[1], CHEN Yue[1], CHANG Zhen-hua[2]
(1. Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004; 2. PLA 69031 Unit, Urumchi 830000)

【Abstract】Aiming at security and privacy threats during Radio Frequency Identification(RFID) tag ownership transfer, this paper proposes a “first delegation then update” ownership transfer mode. Corresponding protocols of the mode are also designed. All the information about the tag is transmitted to the new owner securely after a key negotiation. The tag’s secret is updated securely after a mutual authentication, which makes the old owner can not query the tag any longer. The scheme ensures the privacy and security of the new owner in the ownership transfer.

【Key words】Radio Frequency Identification(RFID); ownership transfer; delegation; key negotiation; security

1 概述

射频识别(Radio Frequency Identification, RFID)技术是20世纪90年代兴起的一种非接触式自动识别技术。凭借其独特优势，RFID技术已在供应链管理、身份识别、交通运输、军事物流等许多领域得到了广泛应用。然而，无线通信固有的安全问题和RFID系统本身存在的一些易受攻击的特性，以及低成本标签的资源限制，使得RFID的安全隐私问题受到了人们越来越多的关注。而RFID标签在其生命周期中进行的所有权转换，又使得这些问题变得更加棘手[1]。

RFID标签生产出来后，制造商将其嵌入商品，再将商品出售给批发商，批发商再卖给零售商，最后消费者再将商品购买，使用一段时间后消费者还可能将商品作为二手物品出售，或由于不满意而退换产品。在这期间的每个环节，都进行了商品的所有权转换。如果用户获得商品所有权后，需要使用RFID标签的功能，享受RFID技术的独特优势，就必须在得到商品的同时，也得到商品上的标签信息。这就涉及到标签的所有权转换问题，即原所有者如何把标签信息传输给新所有者，让新所有者获得标签的控制权，能够对标签进行查询、管理等操作。

但是，如果标签的所有权转换过程只是简单地传输一下相关信息，那么即使新所有者得到了标签的所有权，原所有者仍能利用其所掌握的标签秘密信息，继续对标签进行查询等操作，这就会使得新所有者的安全隐私受到威胁。因为商品的库存、流通、销售等信息一般都属于商业机密，用户携带了哪些物品、处于什么位置，这些也都是用户的个人隐私，而原所有者通过秘密查询就可以获得这些信息。因此，为了保护新所有者的隐私安全，就需要安全地更新标签的秘密信息，保证原所有者虽然拥有标签的相关信息，但其中的秘密信息在标签所有权转换后失效了，不能再对标签进行查询或其他操作，也就不能掌握物品在新所有者处的动态信息。

2 相关工作

RFID标签的所有权转换问题在近几年才逐渐被人们所关注，目前关于这方面的研究还不太多。下面对现有的几个方案进行简要分析。

Molnar等人提出了标签的所有权转换问题[1]，他们设计了一个基于密钥树的假名协议。此协议可以通过2种方法来实现标签的所有权转换：(1)“软失效”，新所有者从可信中心(Trusted Center, TC)获知原所有者被授权了标签的k个假名，则读取标签k+1次，这样原所有者将不能再读取标签。(2)“增加标签计数”，新所有者通过增加标签的计数值，跳过授权给原所有者的那些假名，使得原所有者不能再读取该标签。不过，这2种方法在本质上都只是限时授权，而没有实现完全的所有权转换，新所有者没有完全获得标签的控制权。

Lim等人提出了一个双向认证协议[2]，该协议可以实现完全的所有权转换。协议的基本思想是：在认证过程中，如果认证成功，则用交换的随机数同时刷新标签和数据库的标签秘密；如果认证失败，则标签通过一次Hash计算来更新其秘密。所有权转换过程为，新所有者使用其阅读器，获取标签全部的相关信息，然后，该阅读器用其与标签共享的随机数来刷新标签秘密。该方案对标签的计算能力要求较高，同时，也没有具体说明新所有者如何安全获取标签相关信息。

Fouladgar等人[3]提出了一个简单的所有权转换方案。方案的主要思想为，旧的数据库把标签全部的相关信息都传输

作者简介：邵 婧(1986－)，女，硕士研究生，主研方向：信息管理系统；陈 越，教授、博士；常振华，工程师、硕士

收稿日期：2009-02-15 **E-mail：**shaojingfox@yahoo.com.cn

给新用户的数据库，新用户的阅读器向新数据库发出所有权转换请求，通过验证后，新数据库发出标签秘密更新信息，并由新阅读器转发给标签。此外，文献[4]给出的所有权转换方案没有达到前向安全性和不可跟踪性，文献[5]对其进行了改进。

通过分析发现，现有的所有权转换方案都存在以下问题或其中之一：(1)原所有者仍拥有标签的控制权，没有实现完全的所有权转换；(2)新旧所有者之间如何安全地传输标签的相关信息，没有明确说明。

3 方案描述

3.1 主要思想

通过上述分析可知，一个完全的所有权转换方案，既要保证新所有者能够安全获得标签全部的相关信息，又要保证原所有者不能再对标签进行查询或其他操作，即原所有者不能危害新所有者的隐私安全。同时，方案也要满足 RFID 系统的其他安全性和隐私性需求。根据上述要求，本节提出了一种“先授权后更新”的所有权转换模式，并为模式的 2 个阶段设计了相应的实现协议。

(1)实现对新所有者的阅读器的完全授权，安全地转交标签信息，为所有权转换提供前提保证。为保证方案对无线通信环境的适应性，出于安全考虑，对传输的信息进行加密。然而，一般情况下，新旧所有者之间没有预先共享秘密信息。因此，在发送信息之前双方需要先进行密钥协商，然后再通过协商的密钥把标签全部的相关信息传送给新所有者，实现完全授权。

(2)更新标签秘密信息，完成标签所有权转换。新所有者的阅读器得到授权后，成为了一个临时的后端服务器。阅读器与标签进行双向认证后，更新标签秘密。该秘密更新过程，在实现所有权转换的同时，也满足了 RFID 系统的前向安全性、不可跟踪性、抗重放攻击等安全需求。

3.2 假设

由于成本和大小的限制，因此标签的计算资源和存储空间都非常有限。本文仅假设标签有一个单向 Hash 函数，一个伪随机数发生器，有一定的存储空间和基本的运算能力。同时，一般需要进行所有权转换的标签，其所对应的物品价值都较高，标签成本也不会太低，所以，上述假设是合理的。

新用户的阅读器对应有一个口令，为该用户所有，可以证明用户的合法身份。

3.3 系统初始化

后端服务器选取一个强的大素数β,即至少存在一个大素数因子γ,使β=2γ+1。α为 GF(β)的生成元。α, β在系统中公开。

为简化描述，用 S 代表原所有者的后端服务器，R 代表新所有者的阅读器，T 代表标签。

3.4 授权阶段

授权阶段大致可以分为授权请求、密钥协商和信息传输这 3 个过程。同时，因为同一用户的后端服务器与阅读器之间的通信一般都是安全的，可以把两者视为一个实体，所以本文在授权阶段没有特别指出原所有者的阅读器，但其实 S 与 R 之间还有一个原所有者的阅读器，用于转发消息。

3.4.1 授权请求

(1)$R\rightarrow S$: Delegation, ID_R。新用户使用 R，向 S 发送请求 Delegation 和 R 的身份 ID_R。此处的 ID_R 只是用于识别 R 的身份，并不用于验证。

(2)$S\rightarrow R$: ACK。S 收到消息后，判断出这是一个授权请求，如果此时系统允许，则给出响应 ACK。

(3)R 收到响应后，用户按照提示在购买处手动输入 R 的口令 P，安全地传递给 S。P 和 ID_R 将共同用于随后的密钥协商过程，保证只有同时拥有 P 和 ID_R 的合法用户才能得到正确的协商密钥。

3.4.2 密钥协商

本文采用加密密钥交换(Encrypted Key Exchange, EKE)协议[6]来实现 S 与 R 的密钥协商。EKE 在协议中同时使用了对称密码和公开密钥密码，克服了这 2 种密码系统单独使用时的缺陷，起到了一种秘密放大器的作用。不过，EKE 在使用时，要求协商的双方共享一个口令，而且用口令加密传输的消息必须与随机数不可区分，否则攻击者可以利用消息中的冗余来进行穷举攻击，破解口令，失去协议的优势。具体实现 EKE 采用 Diffie-Hellman 密钥交换协议，如图 1 所示。

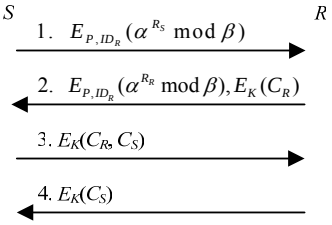

图 1 密钥协商

(1)S 生成一个随机数 R_S，计算 $\alpha^{R_S} \bmod \beta$，并用 P 和 ID_R 对其加密，以克服 Diffie-Hellman 协议容易受到中间人攻击的弱点。S 将 $E_{P,ID_R}(\alpha^{R_S} \bmod \beta)$ 发送给 R。

(2)R 收到消息 1 后，用 P 和 ID_R 对其解密，得到 $\alpha^{R_S} \bmod \beta$。然后，R 生成一个随机数 R_R，计算 $\alpha^{R_R} \bmod \beta$ 和密钥 $K = \alpha^{R_S R_R} \bmod \beta$。而后，$R$ 生成一个随机串 C_R，并用 K 加密。R 将 $E_{P,ID_R}(\alpha^{R_R} \bmod \beta), E_K(C_R)$ 发送给 S。

(3)S 收到消息 2 后，用 P 和 ID_R 解密第 1 部分，得到 $\alpha^{R_R} \bmod \beta$，并计算密钥 $K = \alpha^{R_S R_R} \bmod \beta$。然后，用得到的密钥解密其余信息，得到随机串 C_R。S 生成一个随机串 C_S，将 C_R 和 C_S 用 K 加密后发送给 R。

(4)R 解密消息 3，若得到的 C_R 与之前 R 发送的 C_R 相同，则证明 S 知道 K。用 K 加密得到的 C_S，然后发送给 S。

(5)S 对收到的 $E_K(C_S)$解密，若得到的 C_S 与其发送的 C_S 相同，则证明 R 知道 K，从而完成密钥协商。

3.4.3 信息传输

密钥协商成功后，S 用 K 加密标签的全部相关信息 Info(T)，将 E_K(Info(T))发送给 R。信息中包含 T 与 S 的共享秘密 K_T。

3.5 所有权转换阶段

用户的阅读器得到授权后，就成为了一个暂时的后端服务器，可以与标签直接执行双向认证协议，安全地更新标签秘密信息，实现完全的所有权转换。因为原所有者也掌握标签的秘密信息，也能解密该认证过程，所以该阶段的执行应在原阅读器的读取范围之外进行，这样原所有者就无法获得新的标签秘密。带秘密更新的认证过程如图 2 所示。

(1)R 生成一个随机数 N_R，向 T 发送查询消息{Query, N_R}。其中，N_R 用于防止假冒阅读器对标签的重放攻击。

(2)T 收到查询消息后，生成一个随机数 N_T，并计算 $H(K_T \oplus N_R \oplus N_T)$，其中，$K_T$ 是标签预先存储的秘密信息。T 向 R 发送$\{N_T, H(K_T \oplus N_R \oplus N_T)\}$。随机数 N_T 可以防止标签被跟踪。

(3)R 收到消息 2 后，用 N_T 和 N_R 匹配其数据库中所有标签的 K_{Ti}，看是否存在 $H(K_{Ti}\oplus N_R\oplus N_T)=H(K_T\oplus N_R\oplus N_T)$。如果存在这样的 K_{Ti}，则 T 通过认证。R 生成一个新密钥 K'_T，同时暂时保留原密钥 K_T。然后将$\{K'_T\oplus H(K_T),\ H(K_T\oplus K'_T\oplus N_T)\}$发送给 T。信息的第 1 部分用于恢复出新密钥 K'_T，第 2 部分用于检验恢复出的 K'_T 是否正确。

(4)T 收到消息 3 后，通过 K_T 恢复出 K'_T，并用 $H(K_T\oplus K'_T\oplus N_T)$验证 K'_T 正确与否。如果验证通过，则 T 将其存储的密钥 K_T 更新为 K'_T。并向 R 发送 $H(K_T\oplus K'_T\oplus N_R\oplus N_T)$，表明 T 正确收到了新密钥。

(5)R 收到消息 4 后，对 T 做进一步认证。认证通过后，R 将其数据库中对应标签的密钥 K_T 更新为 K'_T。

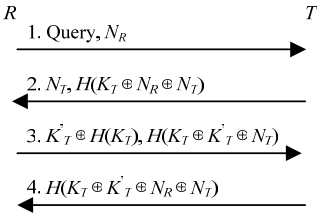

图 2　秘密更新

4　安全性分析

4.1　授权阶段

该阶段实现了完全的授权，用户安全获得了标签的全部相关信息。在授权请求过程，将 R 的口令通过手动输入方式安全地传递给了 S，给密钥协商提供了前提条件。之后的密钥协商过程，满足 EKE 协议的执行条件，传输的信息都是随机数，攻击者若通过穷举攻击来破解口令是十分困难的，而用来生成密钥的信息又受到了口令的加密保护，免受中间人攻击，保证了协商的密钥的安全。标签的全部相关信息是用协商的密钥加密传输的，在不安全的无线通信环境下仍然能够保证信息的安全。

4.2　所有权转换阶段

该阶段使得原所有者失去了标签的控制权，实现了完全的所有权转换。同时也满足标签和阅读器的其他安全需求，实现了安全的转换。该秘密更新协议是一个完整的双向认证协议，可以用于一般的 RFID 系统中的阅读器与标签的查询认证。

所有权转换的完全性：实现了标签所有权的完全转换。方案安全地更新了标签的秘密信息，使得原所有者无法再对标签进行查询或其他操作，新用户完全掌握了标签的所有权。

不可跟踪性：攻击者无法对标签实施跟踪。标签对阅读器的响应中含有随机数，即使攻击者假冒合法的阅读器，不断向标签发送相同的查询信息，标签每次给出的响应也是不同的，所以，攻击者无法判断其收到的响应是否来自同一标签，也就不能对标签实施跟踪。

前向安全性：即使标签当前的密钥 K'_T 被泄露，攻击者也不能得到标签之前的密钥信息 K_T。因为标签秘密每次认证后都进行更新，而且阅读器发送新密钥时，是用$\{K'_T\oplus H(K_T)\}$传送的，所以攻击者通过 K'_T 只能得到 $H(K_T)$，而不能得到 K_T。

抗重放攻击：攻击者对标签和阅读器的重放攻击都将失效。若攻击者将某个合法阅读器的查询重复发送，他也不能得到任何有用的信息，因为标签每次的响应都是不同的。而且攻击者也不能通过重复发送某个合法标签的响应来假冒合法标签，因为阅读器每次发送的查询都是不同的，重复发送上次的响应是无法通过认证的。

4.3　与现有方案的比较

下面将本文方案与现有的一些方案进行比较，如表 1 所示。其中，×表示不满足；√表示满足。

表 1　与现有方案的比较

方案	所有权转换的完全性	不可跟踪性	前向安全性	抗重放攻击	标签信息传输的安全性
文献[1]方案	×	√	×	√	√
文献[2]方案	√	√	√	√	×
文献[3]方案	√	√	√	√	×
文献[4]方案	×	×	×	×	√
文献[5]方案	×	√	√	√	√
本文方案	√	√	√	√	√

比较结果显示，本文所提出的方案克服了现有方案存在的攻击弱点，在达到良好的安全性的同时，实现了所有权转换的完全性和标签信息传输的安全性。

5　结束语

RFID 标签在其生命周期中，如果所有权转换过程不安全，则会给用户的安全隐私带来威胁。本文提出了一种“先授权后更新”的所有权转换模式，并设计了具体的实现协议，实现了安全完全的所有权转换。与现有一些方案的安全性比较表明，本文的方案具有较好的安全性，在所有权转换的完全性和标签信息传输的安全性方面具有一定的优势。

参考文献

[1] Molnar D, Soppera A, Wagner D. A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags[C]//Proc. of SAC’05. Kingston, Jamaica: Springer-Verlag, 2005: 276-290.

[2] Lim C H, Kwon T. Strong and Robust RFID Authentication Enabling Perfect Ownership Transfer[C]//Proc. of ICICS’06. North Carolina, USA: Springer-Verlag, 2006: 1-20.

[3] Fouladgar S, Afifi H. An Efficient Delegation and Transfer of Ownership Protocol for RFID Tags[C]//Proc. of the 1st International Workshop on RFID Technology. Vienna, Austria: [s. n.], 2007.

[4] Osaka K, Takagi T, Yamazaki K, et al. An Efficient and Secure RFID Security Method with Ownership Transfer[C]//Proc. of CIS’06. [S. 1.]: Springer-Verlag, 2007: 778-787.

[5] Lei Hong, CAO Tianjie. RFID Protocol Enabling Ownership Transfer to Protect Against Traceability and DoS Attacks[C]//Proc. of ISDPE’07. Chengdu, China: [s. n.], 2007: 508-510.

[6] Bellovin S M, Merritt M. Encrypted Key Exchange: Password-based Protocols Secure Against Dictionary Attacks[C]//Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy. Oakland, USA: [s. n.], 1992: 72-84.

编辑　索书志