文章编号:2095-476X(2014)05-0052-04

一种可选模式的RFID标签所有权转移协议

甘勇, 杨佳佳, 李天豹

(郑州轻工业学院 计算机与通信工程学院, 河南 郑州 450001)

摘要:针对RFID标签所有权转换过程中的安全、隐私问题,尤其是其中的所有者的授权恢复问题,提出了一种可选模式的RFID标签所有权转移协议.该协议使用阅读器的口令加密信息,在认证方面加强了标签信息的保护.原所有者在释放所有权之后可选择是否申请恢复授权,如果申请成功,可在其使用完标签信息之后的规定时间内释放对标签的所有权,从而保护标签信息的安全和隐私.分析结果表明,该协议提高了标签所有权转换的安全性和灵活性,算法性能也具有一定的优势.

关键词:射频识别;所有权安全转换;可选模式;恢复授权

中图分类号:TP309 **文献标志码**:A DOI:10.3969/j.issn.2095-476X.2014.05.012

A new ownership transfer protocol with optional mode for RFID tags

GAN Yong, YANG Jia-jia, LI Tian-bao

(*College of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou* 450001, *China*)

Abstract: Aiming at the problem of security and privacy in RFID tag ownership transfer, particularly the owner's authorization recovery problem, a RFID tag ownership transfer protocol based on an optional model was proposed. The protocol used the reader's password to encrypt information, and strengthen the certificate protection of label information. After releasing the ownership, the original owner could choose whether to apply for reinstate authorization. If the application was successful, it could allow it to release the ownership after it finished the use of label information within the specified time to protect the security of privacy. The results showed that the protocol improved the security and flexibility of the tag ownership transfer, algorithm performance also had certain advantage.

Key words: RFID; ownership secure transfer; optional mode; reinstate authorization

0 引言

射频识别(RFID)技术是一种感知技术,它是将跨学科的不同专业技术综合在一起的非接触式的自动识别技术.然而,RFID的安全和隐私问题是影响RFID广泛应用的重要因素之一,如RFID标签的所有权转换问题[1].在RFID标签的生命期内,携带标签的商品会通过不同的供应链节点企业.在此过程中,RFID标签的所有者在不断变化,但这些所有者之间并不完全相互信任,他们需要保护各自的商业机密.这就涉及RFID标签所有权转换的安全和隐私问题,比如标签的前向安全、后向安全和授权恢复等,这些都是RFID标签在所有权转换过程中亟待解决的问题.

收稿日期:2014-04-22

作者简介:甘勇(1965—),男,湖南省株洲市人,郑州轻工业学院教授,博士,主要研究方向为分布式计算机系统、计算机网络.

目前,针对这些问题,国内外都有一定的研究. K. Osaka 等[2]提出了一种带有可信第三方的所有权转换协议,该协议使用了 Hash 函数和由密钥控制的加密函数,但无法抵御去同步化攻击. 邵婧等提出了先授权后更新的转换协议[3]和基于公钥密码体制的转换协议[4],虽然这 2 个所有权转换协议都有一定的进步,但它们都无法抵御去同步化攻击,也无法进行授权恢复. H. Wang 等[5]提出了一种新的授权 RFID 标签所有权转移认证协议,该协议不仅保护了标签信息的前向、后向安全,还抵御了拒绝服务攻击,并且能够进行原所有者的授权恢复,但它并没有让用户拥有可选择的权利.

鉴于此,本文提出一种基于可选模式的 RFID 标签所有权转移协议,以提高标鉴所有权转换过程的安全性和灵活性.

1　设计思想

要设计的是一个完全的所有权转移协议:既要保证新所有者能够安全获取标签的信息,又要保证原所有者不能再对标签进行查询等操作;当原所有者需要时,还可以提出授权恢复请求,从而实现授权恢复功能. 根据上述要求,该协议主要从以下 2 个方面进行设计:

1)基于可信第三方的认证阶段. 在从事所有权转移操作前,读取器和标签必须互相验证. 通过引入可信的第三方服务器来监视和控制所有权转移的过程.

2)原所有者的授权恢复. 在所有权转移时,原所有者可以选择是否保留控制权:如果其释放所有权,以后再需要时,如何能恢复授权;如果直接保留控制权,则不能保证所有权转换后标签的后向安全. 因此,应该让原所有者先释放所有权,如果需要恢复授权再设计可选模式的所有权转换协议.

2　协议描述

2.1　假设

基于计算资源有限的特点,假设标签拥有 1 个伪随机数发生器,以便在发送消息时生成随机数来抗重放攻击,还要有 1 个单向的哈希函数,同时拥有特定的存储空间和基本计算能力. 另外,申请授权所有者的阅读器需要对应有 1 个口令,用来证明所有者的身份合法.

2.2　初始化

引入 1 个可信的第三方(TC)服务器来进行管理,并有权决定是否对申请者进行授权. 每个潜在用户必须先在 TC 注册自己的身份. TC 和每个标签 T_i 共享 1 个密钥 K_{T_i},K_{T_i}预先装到 T_i 的私有内存空间里,只有 *TC* 和 T_i 知道和有权访问这个密钥. 同样,当前的所有者阅读器 R_j 和 T_i 也有 1 个共享密钥 K_{R_j}. 此外,每个 R_j 还拥有 1 个凭证密钥 C_{R_j}.

2.3　授权阶段

授权阶段的协议设计如图 1 所示.

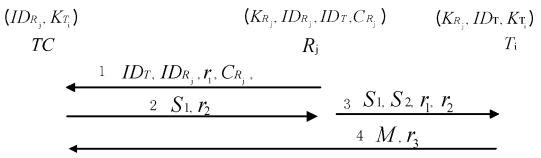

图 1　授权阶段

首先,当前所有者向 *TC* 发送授权请求. 在收到授权请求时,*TC* 将首先验证当前所有者的身份. 同时 *TC* 为所有者的标签生成一个临时密钥,然后构造一条新消息将临时密钥发送给当前所有者. 收到消息后,当前所有者用标签和自己共享的密钥构造另一条消息,将其连同 *TC* 的消息一起发送给标签. 标签通过计算获得临时密钥,再构造新消息将临时密钥和标签与 *TC* 的共享密钥一起发送给 *TC*. *TC* 收到消息后,验证该临时密钥若是自己生成的密钥,则授权给当前所有者.

2.4　所有权转换阶段

该阶段参照文献[3]. 具体的所有权转移过程如图 2 所示.

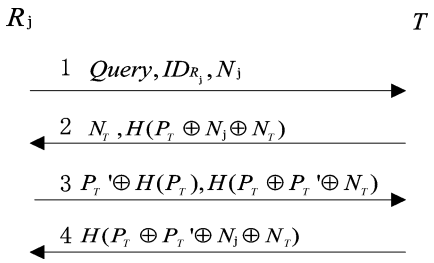

图 2　所有权转换阶段

当前所有者的阅读器和标签首先进行双向身份认证,认证成功之后,当前所有者的阅读器再进行密钥更新,使原所有者无法再对标签进行查询等操作,从而实现了标签所有权的转换.

2.5 授权恢复阶段

授权恢复阶段是本文设计协议的重点,主要由2个部分实现,即认证阶段和授权恢复阶段. 当前所有者首先验证原所有者 R_i 的身份. 验证通过后,通过1个标记值 Q 来表示所有者不同意或同意标签所有权转换($Q=0$ 或1). 当前所有者和原所有者分别拥有 Q_j 和 Q_i,只有当 Q_i 和 Q_j 同时为1时,原所有者才有可能恢复标签的所有权,其他任何情况都不能恢复对标签的所有权. 为了使标签的安全和隐私切实受到保护,增加1个计时器来控制授权恢复过程,该计时器由当前所有者控制. 具体的实现过程如图3所示.

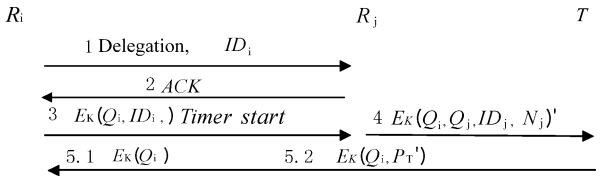

图3 授权恢复阶段

1)$R_i \rightarrow R_j$:首先,R_i 向 R_j 发送一个授权恢复请求,并发送自己的身份 ID,以防止中间人攻击.

2)$R_j \rightarrow R_i$:R_j 收到 R_i 的消息后,判断它是否为一个合法的授权请求(前面已经提到,申请授权所有者的阅读器需要对应有一个口令,用来证明所有者的身份合法). 如果允许,R_j 将给出 ACK 回应,并在屏幕上给出输入 R_i 的口令 P_i 的提示信息.

3)$R_i \rightarrow R_j$:R_i 收到 ACK 后,在屏幕上输入自己的口令 P_i,当屏幕上显示"授权请求成功"时,让原所有者进行选择,并将选择的结果 Q_i 加密后发送给 R_j. 与此同时,当前所有者开启计时器.

4)$R_j \rightarrow T$:R_j 收到消息后进行判断,如果 $Q_i=1$,则 R_j 显示提示信息让当前所有者设置 Q_j 的值,如果 $Q_j=1$,表明当前所有者允许原所有者恢复所有权. 然后 R_j 将 Q_i 和 Q_j 以及自己的身份 ID 加密后发送给 T.

5)$T \rightarrow R_i$:T 收到消息后,将消息解密并进行判断,如果 Q_i 和 Q_j 都为1,则 T 将 Q_i 和 P_T' 加密后发送给 R_i,否则,T 就只发送 Q_i.

原所有者解密后得到 P_T',并不代表授权恢复成功,这时就体现了计时器的作用:原所有者得到 P_T' 后,如果在规定时间内没有释放所有权,即到达规定的时间 Q_i 仍然是1,则显示超时并且当前所有者强制使 $Q_i=0$,让原所有者释放所有权,并重新开始步骤3);如果在规定时间内原所有者修改 $Q_i=0$,则表明原所有者在规定时间内完成了对标签的使用并释放了所有权,表明原所有者整个授权恢复过程成功完成.

3 安全性分析

1)抗中间人攻击:在授权、所有权转换以及授权恢复这3个过程中,都加入了所有者身份验证的过程,因而攻击者想通过穷举搜索来攻击消息是非常困难的.

2)抗重放攻击:在消息传输的整个过程中,所有者在发送消息时都生成了随机数,而且标签每一次给出的响应也都不同,所以攻击者不可能通过重复发送某个消息而假冒合法标签,也无法通过认证.

3)前向安全性:由所有权转换阶段可知,即使是攻击者获得标签当前的密钥 P_T',它也不能获得标签之前的秘密信息. 因为标签的密钥在每次认证后都进行更新,况且阅读器发送的是 $P_T' \oplus H(P_T)$,即使攻击者拥有 P_T',它也只能通过 P_T' 得到 $H(P_T)$ 而非 P_T. 因此,标签的前向安全得到保护.

4)后向安全性:在授权阶段,通过引入第三方产生一个临时密钥来保护标签的后向安全. 由于该临时密钥只是用来验证所有者的身份而不用于所有权的转移,因此即使原所有者获得了该临时密钥,也不能通过它识别和跟踪标签,标签的后向安全得到保护.

5)不可跟踪性:在所有权转换阶段,标签对阅读器的响应中含有随机数,标签每次给出的响应都不一样,因此,攻击者不能判断出其收到的回应是否来自于同一标签,所以不能对标签进行跟踪.

本协议与现有一些协议的安全性比较如表1所示.

表1 本文协议与现有一些协议的安全性比较

协议	不可跟踪性	前向安全	后向安全	抗重放攻击	抗中间人攻击	可选	可恢复授权
文献[2]	×	×	×	×	√	×	×
文献[4]	√	√	×	√	√	×	×
文献[5]	√	√	√	√	√	×	√
文献[6]	√	√	√	√	√	×	×
文献[7]	√	√	×	√	√	√	×
本文协议	√	√	√	√	√	√	√

注:√表示满足条件,×表示不满足条件.

4　算法性能分析

考虑到 RFID 系统中标签的成本、计算能力及存储能力等关键性因素,笔者将本文协议与现有一些协议进行算法性能的比较,主要比较标签计算 Hash 函数的次数. 比较结果如图 4 所示.

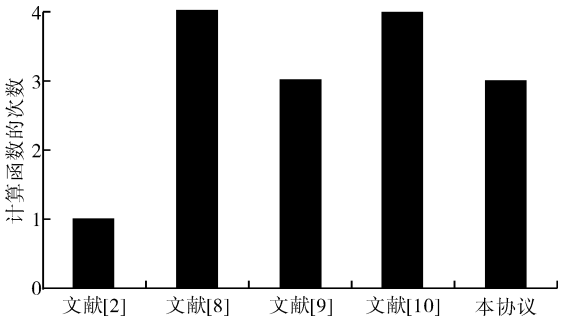

图 4　标签计算 Hash 函数的次数比较

由图 4 可见,本协议中标签计算 Hash 函数的次数相对比较少,运行效率比较高;同时,使用异或、按位 OR 运算以及 Hash 函数的逻辑操作可以在低成本的 RFID 标签上实现. 因此该协议具有一定的可行性.

5　结论

本文针对 RFID 标签所有权转移协议进行了研究,提出了一种可选模式的 RFID 标签所有权转移协议. 该协议满足了所有权转移协议时所有需要的安全和隐私保护,如抵御重放攻击、保护标签隐私的前向、后向安全等. 另外,如果原所有者需要恢复对标签的控制权,可以用本文提供的选择模式进行选择. 当原所有者使用过标签信息之后,系统还可以让其在规定时间内释放对标签的控制权,从而保护标签信息安全. 通过与现有一些协议的比较,本文协议在标签所有权转换的安全性和算法性能方面具有一定的优势.

参考文献:

[1] 贺蕾,甘勇,蔡增玉,等. HB 及相关轻量级认证协议研究[J]. 郑州轻工业学院学报:自然科学版,2008,22(6):91.

[2] Osaka K, Takagi T, Yamazaki K, et al. An efficient and secure RFID security method with ownership transfer [C]// Proceedings of RFID Security, New York: Springer US, 2009: 147.

[3] 邵婧,陈越,甄鸿鹄. 供应链环境下的 RFID 标签所有权转换方案[J]. 计算机工程与设计, 2009, 30(24):5618.

[4] 邵婧,陈越,常振. RFID 标签所有权转换模式及协议设计[J]. 计算机工程,2009,35(15):143.

[5] Wang H, Yang X, Huang Q, et al. A novel authentication protocol enabling RFID tags ownership transfer [C]// Proceedings of 2012 IEEE 14th International Conference on Communication Technology (ICCT), Piscataway: IEEE, 2012: 855.

[6] Fouladgar S, Afifi H. An efficient delegation and transfer of ownership protocol for RFID tags[C]// Proceedings of First International EURASIP Workshop on RFID Technology, Heidelberg: Springer, 2007.

[7] Zhou X I, Wang A, Xi T. A new optional ownership transfer mode of RFID tags[J]. Journal of Information & Computational Science, 2013, 10(8): 2471.

[8] 邵婧. RFID 标签所有权转换机制研究[D]. 郑州:中国人民解放军信息工程大学,2009.

[9] Song B. RFID tag ownership transfer[C]//Proceedings of Workshop on RFID Security 2008, Budapest: [s. n.], 2008.

[10] Dimitriou T. rfidDOT: RFID delegation and ownership transfer made simple[C]//Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks, New York: ACM, 2008: 34.