ISSN 1000-1239/CN 11-1777/TP
48(8): 1400-1405, 2011

RFID 标签所有权转移协议研究

金永明[1,2] 孙惠平[3] 关 志[1,2] 陈 钟[1]
[1](北京大学信息科学技术学院网络与信息安全实验室 北京 100871)
[2](高可信软件技术教育部重点实验室(北京大学) 北京 100871)
[3](北京大学软件与微电子学院 北京 100871)
(yongmingjin@163.com)

Ownership Transfer Protocol for RFID Tag

Jin Yongming[1,2], Sun Huiping[3], Guan Zhi[1,2], and Chen Zhong[1]
[1](*Network & Information Security Laboratory, School of Electronics Engineering and Computer Science, Peking University, Beijing* 100871)
[2](*Key Laboratory of High Confidence Software Technologies (Peking University), Ministry of Education, Beijing* 100871)
[3](*School of Software and Microelectronics, Peking University, Beijing* 100871)

Abstract Radio frequency identification (RFID) is becoming ubiquitous at present, which is suitable for ubiquitous computing environment. Its flexibility holds great promise for novel applications, and increasingly RFID tags are being deployed. RFID security and privacy is the basic requirement in most applications. Conventional security primitives cannot be integrated in RFID tags as they have inadequate computation capabilities with extremely limited resources. Therefore, it is important to have some lightweight security mechanisms suitable for RFID tags. A tagged item will be often passed to a new owner. The privacy of the new (as well as the past) owner should be guaranteed. Based on SQUASH—a message authentication code (MAC) with provable security properties for highly constrained devices, a new lightweight ownership transfer protocol is proposed. The new protocol has more efficient performance than other Hash-based schemes. Moreover, it achieves very strong notion of security and it is the first protocol based on SQUASH whose security properties have been proven. Finally, the new protocol can protect the forward and backward privacy of both parties that is very important requirement in the ownership transfer application.

Key words security; authentication; ownership transfer protocol; RFID; privacy protection technology

摘 要 无线射频识别技术(RFID)是适用于普适计算环境的技术之一,它的应用正在变得随处可见.RFID 安全与隐私问题是这些应用的基本需求之一.由于 RFID 标签的资源限制,传统的安全元素不能很好地应用到 RFID 标签中.因此,设计轻量级的安全机制非常重要.应用中,贴有标签的物品经常发生所有权的转移.这就需要保护原所有者与新所有者的隐私.基于 SQUASH 方案,一种具有可证安全属性的消息认证码机制,提出了一种新的轻量级所有权转移协议.新协议比基于 Hash 的方案具有更高的效率.同时,它还具有很强的安全特性.新协议是第 1 个基于 SQUASH 的方案,优化了所有权转移协

收稿日期:2011-04-07;**修回日期**:2011-06-21
基金项目:国家自然科学基金项目(60773163)

议,去掉了 Hash 方案中不需要的特性.最后,新协议完全满足所有权转移协议的要求,可有效保护原所有者与新所有者的前向与后向隐私.

关键词 安全;认证;所有权转移协议;无线射频识别;隐私保护技术

中图法分类号 TP309

无线射频识别技术(RFID)是一种感知技术,通过电子磁场可以实现信息的自动获取,进而可以识别所标识的物体.它可以自动实现人与物之间,或物与物之间的交互,是普适计算的基础技术之一.同时,RFID 技术也是物联网的核心技术之一,与感应器一起成为构建物联网的基础元素.虽然 RFID 技术已经有几十年的历史,近几年才逐渐获得广泛关注,引发了很多具有广阔前途的应用研究,比如:智能交通、智能医疗、智能城市,甚至智慧地球等等.

RFID 安全与隐私问题是影响 RFID 广泛应用的重要因素之一,获得了普遍的关注.RFID 标签的成本都比较小,可使用的计算能力与存储能力都非常有限.一般情况下,它们只有几百个存储位(bit),和 5 000~10 000 的逻辑门[1].因此,传统的安全元素(比如 RSA,AES 等)都无法直接在 RFID 标签中应用.如何设计轻量级的安全机制,成为 RFID 安全与隐私研究的重点内容之一[2-4].

在 RFID 标签的生命期内,它的所有者经常需要发生改变[5].比如,一个产品生产时贴上 RFID 标签,生产商在产品线对产品进行管理.当产品到批发商时,RFID 标签的所有者由生产商变为批发商,批发商需要对产品的物流过程进行管理.批发商把贴有 RFID 标签的产品转给零售商,则 RFID 标签的所有者变为零售商,零售商要对产品进行库存管理.当顾客购买商品后,RFID 标签的所有者又会变为顾客.若涉及商品的售后服务,则 RFID 标签的所有权会有更多的转移过程.

在 RFID 标签的所有权转移过程中,需要满足以下安全与隐私要求:1)所有权转移后,原所有者不能继续访问 RFID 标签;2)新所有者在获得 RFID 标签的所有权后,不能访问以前 RFID 标签进行的交互数据,以保护原所有者的隐私;3)所有权转移协议可以抵抗中间人攻击、异步攻击等等.

1 相关工作

使用对称密码加密,Saito 等人提出了一种密钥更新方案,可以在所有权转移后防止原所有者继续读取 RFID 标签的数据[6].在该方案中,RFID 标签中的唯一标识 ID 用对称密码进行加密,以防止 ID 信息泄露.当新所有者获得 ID 后,该协议通过可信第三方(TTP)加密新的密钥,完成所有权转移过程.该方案的缺陷是需要引入可信第三方,增加了复杂度.

2005 年,Molnar 等人提出了一个支持 RFID 标签所有权转移的可扩展授权协议[5].该协议具有可扩展性,通过为 RFID 标签提供一个“假名”来保护用户的隐私.通过授权,读写器可以不通过可信中心(TC)就可以为 RFID 标签设置“假名”.另外,该协议也支持与可信实体进行的所有权转移过程.该方案的主要缺点是需要假定原所有者与新所有者有一个共同的可信中心.现实中,限制了该协议的应用范围.

2006 年,Osaka 等人讨论了 RFID 系统的安全需求,基于 Hash 函数和对称密码体制提出了一个新的 RFID 安全机制,可以满足 RFID 系统所需要的安全特性[7].在认证过程中,该协议认证读写器传来的数据,产生 Info(ID)返回给读写器.在所有权转移过程中,通过改变对称私钥,可保护原所有者与新所有者的隐私.然而,该方案也存在一些缺陷:一是该协议不能抵抗拒绝服务(DoS)攻击;二是该协议不满足不可追踪性.攻击者通过使用相同的随机数询问读写器,读写器会返回相同的响应,故攻击者可以对 RFID 标签进行跟踪.

2007 年,Fouladgar 和 Afifi 提出了一个新的协议,可以简化和提高授权协议的安全性[8].同时,提出了一个简单有效的所有权转移方法,可保护 RFID 标签新所有者的隐私.在该协议中,标签只需要存储 K_p,K_u 和计数器,效率比较高.然而,由于 RFID 标签每次返回 K_p 和一个随机数的 Hash 值,而随机数是标签自己产生的,则攻击者可以重复使用该返回值,进而可以冒充该标签.另外,标签使用的私钥 K_p,K_u 并不是每次都更新,因此,容易有被跟踪的威胁.

Jappinen 和 Hamalainen 也提出了一个简单有效的安全机制可以实现所有权转移过程[9].该方案

是基于 Osaka 方案的改进,修正了原方案的一些缺陷,提高了原方案的效率.

2008 年,Song 提出了一个 RFID 所有权转移认证过程,该方案主要包括 3 个子协议:所有权转移协议(P_1)、密钥更新协议(P_2)和授权恢复协议(P_3)[10]. 其中协议 P_1 和 P_2 基于 SM 协议[4]. 执行完协议 P_1 后,服务器 S_{j+1} 则拥有了标签 T 的所有权. 然后 S_{j+1} 执行另一个协议 P_2,更新标签 T 的私钥,来保护新所有者的隐私. 事实上,所有权认证协议没必要分成 2 个子协议来执行. 该协议可以作进一步的优化.

2010 年,Kulseng 等人提出了一个轻量级的 RFID 相互认证协议,只有合法认证的读写器和标签才能相互通信[11]. 在此基础上,又提出了一个所有者转移协议. 新协议使用了物理不可克隆功能(PUF)和线性反馈移位寄存器(LFSR),与基于 Hash 函数的协议相比,效率提高了很多. 但 PUF 的安全性并不像 Hash 函数一样,得到了充分的研究,本文对此不作效率和安全性分析. 从新协议本身而言,该协议需要可信第三方的参与,限制了该协议的应用. 另外,协议是否能抵抗已知的攻击,比如重放攻击、异步攻击等,未进行详细的分析.

2 SQUASH 方案

2008 年,Shamir 提出了一个基于 Hash 函数的优化函数 SQUASH,非常适合基于 RFID 的挑战响应认证方式[12]. SQUASH 方案的基本思想是:减少 Rabin 加密方案的步骤,去掉一些不需要的特征.

该方案描述了如何简化和提高 Rabin 加密方案效率,而不影响 Rabin 著名的单向性. 首先,Rabin 加密方案中使用的 n 不必要是可分解的,因为标签和读写器都不需要分解 n 来解密密文. 其次,方案推荐使用梅森数(2^k-1)来作为 n,这样存储 n 将使用更少的空间. 第三,梅森数作为 n 不仅容易存储,而且更容易计算 n 的模平方运算. 第四,在传输加密密文 c 时,没必要全部传输,可以只传输其中的一部分,同样可以保证方案的安全性. 比如只传输 c 的 32 b,被欺骗的概率已经小于 $1/(4\times10^9)$. 其他细节可以参考文献[11-12].

3 一种新的轻量级所有权转移协议:LOTP

本节提出一种新的轻量级所有权转移协议 LOTP. 首先,我们给出基本的定义.

T_i:进行所有权转移的标签;

R_i:新所有者 RFID 系统的读写器;

D_i:新所有者 RFID 系统的数据库;

D_j:原所有者 RFID 系统的数据库;

k:安全参数;

n:Rabin 加密方案的因子,使用梅森数,$n=2^k-1$;

t:交换密文的长度;

s_i:T_i 长度为 l 的私钥;

t_i:T_i 长度为 l 的公钥,等于 $s_i^2 \bmod n$;

u_i:T_i 前一轮的私钥;

v_i:T_i 前一轮的公钥,等于 $u_i^2 \bmod n$;

U_i:T_i 存储的业务数据;

s_i':T_i 的新私钥;

t_i':T_i 的新公钥,等于 $s_i'^2 \bmod n$;

u_i':T_i 新数据库中存储的上一轮私钥;

v_i':T_i 新数据库中存储的上一轮公钥,等于 $u_i'^2 \bmod n$;

$\oplus$:异或运算;

$[x]_t$:取 x 的 t 位;

$\leftarrow$:置换(赋值)运算;

$x>>a$:右循环移位运算;

轻量级所有权转移协议主要解决读写器与标签之间无线传输的安全与隐私问题,因此不失一般性,假设读写器与数据库之间有安全的通信信道. 同时,新所有者的数据库与原所有者的数据库之间也有可信的通信信道. 协议的过程如图 1 所示.

主要分为 6 个步骤:

1) $R_i \rightarrow T_i$.

读写器向标签发起请求消息.

2) $T_i \rightarrow R_i \rightarrow D_i \rightarrow D_j$:$M, N$.

标签选择一个随机数 r_T,计算 $M=t_i \oplus r_T$,$N'=r_T^2 \bmod n$,$N=[N']_t$,然后把($Query$,M,N)发送给新所有者的读写器,读写器再把(M,N)传给新所有者的数据库. 新所有者的数据库把数据通过安全信道传给原所有者的数据库.

3) $D_j \rightarrow D_i$:(s_i, t_i),U_i.

对原所有者数据库中的(s_i, t_i)对,D_j 计算$N'=(M \oplus t_i)^2 \bmod n$ 并验证是否存在 $N=[N']_t$. 如何能找到一条记录使等式成立,则标签 T_i 认证通过,是一个合法的标签. 然后 D_j 把标签的公私钥对(s_i, t_i)和数据 U_i 通过安全通道发送给 D_i. 这时,D_i 已经获得标签 T_i 的所有权授权. 若未找到记录可以使等式成立,根据不同的效率与安全折中策略,分为以

下 2 种情况(本文按后一种情况讨论):一是为了保证强安全性,D_j 停止协议过程,所有权转移过程未通过;另一是为了效率和抗异步攻击,D_j 计算 $N'=(M\oplus v_i)^2 \bmod n$,并验证是否存在一条记录使得 $N=\lfloor N'\rfloor_t$. 若能找到,D_j 用 (u_i,v_i) 代替 (s_i,t_i),和 U_i 一起发送给 D_i. 若未找到,则停止协议过程,所有权转移过程未通过.

4) $D_i \rightarrow R_i: P,Q$.

为了向标签 T_i 认证并更新标签 T_i 的公私钥,D_i 选择一个随机数 $s_i' \in_R \{0,1\}^l$,计算 $t_i'=s_i'^2 \bmod n$,则 (s_i',t_i') 成为标签 T_i 新的公私钥对. 然后 D_i 计算 $r_T=M\oplus t_i$, $P=t_i'\oplus(r_T>>l/2)$, $Q=s_i\oplus(t_i'>>l/4)$,把 P,Q 发送给 R_i. 最后,D_i 更新存储的上一轮公私钥对,把 (u_i,v_i) 替换为 (s_i,t_i),并保存新的公私钥对 (s_i',t_i').

5) $R_i \rightarrow T_i: P,Q$.

读写器 R_i 把 P,Q 发送给标签 T_i.

6) 标签:T_i.

标签 T_i 计算 $t_i'=P\oplus(r_T>>l/2)$, $Q'=s_i\oplus(t_i'>>l/4)$. 如果 Q' 等于 Q,则把 t_i 替换为 t_i'.

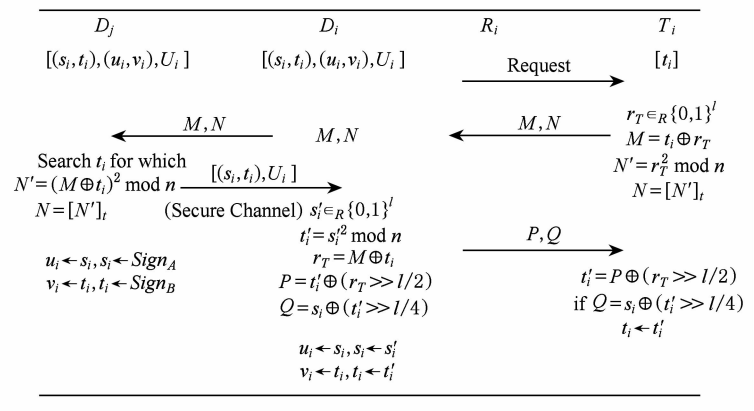


Fig. 1 Lightweight ownership transfer protocol: LOTP.

图 1 轻量级所有权转移协议 LOTP

4 安全与效率分析

下面我们对新协议的安全性与隐私进行简要分析.

重放攻击(RA):新协议可以抵抗重放攻击. 若攻击者使用旧的消息 (M,N),攻击者需要找出一个 t_i 满足 $N'=(M\oplus t_i)^2 \bmod n$, $N=\lfloor N'\rfloor_t$,而攻击者是无法解密 SQUASH 密文的.

异步攻击(DoS):为了抵抗异步攻击(可理解为拒绝服务攻击的一种),新协议设计存储了上一轮认证的公私钥用来实现与 T_i 恢复同步. 如果攻击者阻止了消息 P,Q 发送给 T_i,T_i 则不会更新存储的公私钥. 但是 D_i 会继续协议过程,更新了自己的公私钥. 这就造成了异步. 在新协议过程中,T_i 将使用上一轮公私钥计算 M,N,则 D_i 能从上一轮公私钥中恢复 (u_i,v_i),顺利完成认证过程.

中间人攻击(MITM):因为读写器与标签之间是无线传输,任何攻击者都可以获得消息 (M,N) 和 (P,Q). 攻击者可以替换消息,对消息进行修改等等. 若攻击者替换或修改了消息,则他需要找到一个 t_i 满足等式 $N=(M\oplus t_i)^2 \bmod n$, $N=\lfloor N'\rfloor_t$,否则在下一步认证时就无法通过.

可证安全(PS):如上所述,新所有权转移协议的安全性取决于 SQUASH 的安全性. 而 SQUASH 的安全性可归结为 Rabin 加密体制的安全性,是可证安全的. 对任意选定的消息 M, $SQUASH(M(S,R))$,它的安全性不低于消息 $Rabin(M(S,R))$ 的安全性.

前向隐私(FP):新协议可以保护原所有者的隐私. 在所有权转移过程中,新所有者可以获得原所有者每次交互的 (s_i,t_i) 和 U_i. 由于原所有者每次使用 Rabin 加密体制更新公私钥 (s_i,t_i),新所有者若想获得原所有者的隐私,则需要解密 Rabin 加密密文.

后向隐私(BP):新协议可以保护 T_i 新所有者的隐私. 由于新所有者更新了公私钥 (s_i',t_i'),攻击者,甚至原所有者都不能识别新所有者与标签 T_i 之间的交互过程. 因为他们无法计算出一个 t_i' 满足 $N'=(M\oplus t_i)^2 \bmod n$, $N=\lfloor N'\rfloor_t$,不能再访问 T_i.

表 1 给出了新协议与常见的所有权转移协议之间的安全特性比较.

Table 1 Comparison of Security and Privacy of Ownership Transfer Protocol

表 1 所有权转移协议安全性与隐私比较

Schemes	FP	BP	RA	DoS	MITM
Osaka[7]	×	×	√	×	√
Fouladgar[8]	×	√	√	×	√
Jappinen[9]	*	√	√	×	√
Song[10]	*	√	√	√	√
The new scheme	*	√	√	√	√

√: provided; *: provided under an assumption; ×: hot provided.

假设所有权转移协议中,密钥的长度为 l,则标签需要 l 比特的空间存储 t_i. 另外,标签 T_i 需要 k 位存储 n,用于计算 SQUASH 加密密文.

在所有权转移协议中,首先读写器会发送一个随机数给标签,然后继续下边的认证过程. 新协议简化了这个过程,只需要发送一个请求即可. 以 Song 等人的方案为例,对于标签 T,它能够计算 $r'=r_2-r_1$,然后代替 r_2. 因为 r_1 是可被随意获取的明文,所以多发一个随机数并不能提高安全性和消息(M_1, M_2)的随机性.

显然,新协议与其他方案相比,需要后端数据库更多的存储空间来存储上一轮的公私钥(u_i, v_i),来抵抗异步攻击. 一般来说,后端数据库的存储能力都是非常大的,所以从效率和安全性折中考虑,是可行的.

表 2 给出了所有权转移协议的计算、存储与通信代价的比较. h 是 Hash 函数计算代价,p 是异或运算代价,q 是位移运算代价,l 是 T_i 的密钥长度,t 是交换密文长度.

Table 2 Comparison of Efficiency of Ownership Transfer Protocol

表 2 所有权转移协议效率比较

Schemes	TC	TS	CC
Osaka[7]	$h+2p$	l	$3l$
Fouladgar[8]	$h+5p$	$2l$	$5l$
Jappinen[9]	$2h+5p$	l	$4l$
Song[10]	$6h+9p+4q$	l	$9l$
The new scheme	$2k+3p+2q$	$l+k$	$2l+2t$

TC: tag computation; TS: tag storage; CC: communication cost.

5 结 论

本文对 RFID 标签所有权转移协议进行了研究,提出了一个新的基于 SQUASH 的所有权转移协议. 新协议满足所有权转移协议所需要的安全特性,比如重放攻击、中间人攻击等等,而且能保护原所有者与新所有者的隐私. 新方案是第 1 个基于 SQUASH 的所有权转移协议,与已知的基于 Hash 函数的方案相比,在计算、通信能力上效率更高. 为了抵抗异步攻击,新协议需要额外存储上一轮的公私钥. 一般来说,后端数据库的存储能力都是非常大的,所以从效率和安全性折中考虑,在现实中是可行的.

致谢 研究工作得到了网络与信息安全实验室老师和 RFID 安全与隐私研究小组同学的支持和帮助,在此表示衷心的感谢!

参 考 文 献

[1] Juels A, Weis S A. Authenticating pervasive devices with human protocols [G] //LNCS 3621: Proc of Advances in Cryptology—CRYPTO 2005. Berlin: Springer, 2005: 293-308

[2] Zhou Yongbin, Feng Dengguo. Design and analysis of cryptographic protocols for RFID [J]. Chinese Journal of Computers, 2006, 29(4): 581-589 (in Chinese)
(周永彬, 冯登国. RFID 安全协议的设计与分析[J]. 计算机学报, 2006, 29(4): 581-589)

[3] Ding Zhenhua, Li Jintao, Feng Bo. Research on Hash-based RFID security authentication protocol [J]. Journal of Computer Research and Development, 2009, 46(4): 583-592 (in Chinese)
(丁振华, 李锦涛, 冯波. 基于 Hash 函数的 RFID 安全认证协议研究[J]. 计算机研究与发展, 2009, 46(4): 583-592)

[4] Song B, Mitchell C J. RFID authentication protocol for low-cost tags [C] //Proc of ACM Conf on Wireless Network Security—WiSec'08. New York: ACM, 2008: 140-147

[5] Molnar D, Soppera A, Wagner D. A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags [G] //LNCS 3897: Proc of Selected Areas in Cryptography—SAC 2005. Berlin: Springer, 2005: 276-290

[6] Saito J, Imamoto K, Sakurai K. Reassignment scheme of an RFID tags key for owner transfer [G] //LNCS 3823: Proc of Embedded and Ubiquitous Computing—EUC 2005 Workshops. Berlin: Springer, 2005: 1303-1312

[7] Osaka K, Takagi T, Yamazaki K, et al. An efficient and secure RFID security method with ownership transfer [G] //LNCS 4456: Proc of Computational Intelligence and Security—CIS 2006. Berlin: Springer, 2006: 778-787

[8] Fouladgar S, Afifi H. An efficient delegation and transfer of ownership protocol for RFID tags [C] //Proc of the 1st Int EURASIP Workshop on RFID Technology. Piscataway, NJ: IEEE, 2007: 10-14

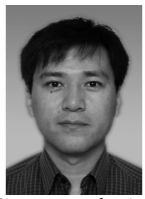
[9] Jappinen P, Hamalainen H. Enhanced RFID security method with ownership transfer [C] //Proc of 2008 Int Conf on Computational Intelligence and Security. Piscataway, NJ: IEEE, 2008: 382-385

[10] Song B. RFID tag ownership transfer [C/OL] //Proc of the Conf on RFID Security. 2008. [2011-04-01]. http://event.iaik.tugraz.at/RFIDSec08/Papers

[11] Kulseng L, Yu Zhen, Wei Yawen, et al. Lighteweight mutual authentication and ownership transfer for RFID systems [C] //Proc of the 29th Conf on Computer Communications—IEEE INFOCOM 2010. Piscataway, NJ: IEEE, 2010: 1-5

[12] Shamir A. SQUASH—A new MAC with provable security properties for highly constrained devices such as RFID tags [G] //LNCS 5086: Proc of the 15th Annual Fast Software Encryption Workshop. Berlin: Springer, 2008: 144-157

Jin Yongming, born in 1979. PhD candidate at Peking University. His current research interests include digital signature, authenticaton protocol, privacy protection technology, etc.



Sun Huiping, born in 1975. Assistant professor from 2005 in the School of Software and Microelectronics, Peking University, China. Member of IEEE, ACM and China Computer Federation. His research interests mainly include identity and trust management, RFID security and privacy, social network and P2P security.

Guan Zhi, born in 1980. Received his PhD degree from Peking University. Assistant professor in Peking University. His current research interests include cryptography and system security.

Chen Zhong, born in 1963. Professor at Peking University. Senior member of China Computer Federation. His current research areas include network security and software engineering.