第35卷 第21期 计 算 机 工 程 2009年11月
Vol.35 No.21 Computer Engineering November 2009
·安全技术· 文章编号：1000—3428(2009)21—0138—02 文献标识码：A 中图分类号：TP309

基于Hash锁的同步强化RFID验证协议

白 煜[1]，滕建辅[1,2]，张立毅[1,2]，郭继昌[1]
(1. 天津大学电子信息工程学院，天津 300072；2. 天津商业大学信息工程学院，天津 300134)

摘 要：针对基于Hash函数和密钥更新机制的无线射频识别(RFID)安全协议可能导致数据同步，使得标签认证失败的问题，对几种RFID安全协议保护同步的方法进行分析，指出它们的特点和局限，在此基础上提出基于Hash锁的同步强化RFID安全协议。该协议在数据库记录中添加保护数据同步的密钥K_p，解决了数据同步问题。分析结果表明该协议实现了防止信息泄露、不可追踪性和数据同步等要求，且计算复杂度低。

关键词：无线射频识别；隐私安全；同步；Hash锁

Hash Lock-based Strengthen Synchronization RFID Authentication Protocol

BAI Yu[1], TENG Jian-fu[1,2], ZHANG Li-yi[1,2], GUO Ji-chang[1]
(1. School of Electronic Information Engineering, Tianjin University, Tianjin 300072;
2. College of Information Engineering, Tianjin University of Commerce, Tianjin 300134)

【Abstract】The Radio Frequency Identification(RFID) authentication protocol based on Hash lock and key updating may lead to desynchronization which makes the tag-to-reader authentication fall into failure. In the paper, the anti-desynchronization methods of several RFID authentication protocols are analyzed and the disadvantages of which are also pointed out, and a novel scheme, Hash lock-based strengthen synchronization RFID authentication protocol is proposed. The scheme achieves the anti-desynchronization requirement by adding anti-desynchronization Key K_p into the database. Analysis result shows that the new scheme realizes the requirement of anti-information leakage, intraceability and synchronization with a low computing load.

【Key words】Radio Frequency Identification(RFID); privacy security; synchronization; Hash lock

无线射频识别(Radio Frequency Identification, RFID)是一种非接触自动识别技术，具有视距/非视距识别、读取速度快、适应恶劣工作环境等优点。然而，隐私和安全问题制约了RFID技术的广泛应用。RFID隐私安全问题源于RFID标签的基本功能，即任意一个标签都能在远程被任意地扫描，并自动响应问询。这一功能可以被用来追踪特定的用户或物品，获得相关隐私信息，例如对标签的非法跟踪侵犯了标签持有者的位置隐私。

1 RFID技术及其隐私安全分析

1.1 RFID系统介绍

RFID系统主要由标签、读写器和数据库组成，如图1所示。

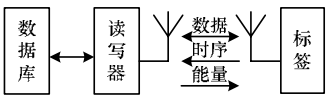

图1 RFID系统的基本组成

为了获得标签的数据，首先读写器向标签发射电磁波能量和问询命令；标签获得能量后将标签的标识信息发送给读写器；读写器根据接收到的标识查询后端数据库获得标签的相关信息。RFID技术已应用于物流、门禁、宠物跟踪、电子钱包、高速公路收费等领域，有望代替条形码。

1.2 隐私安全问题

RFID安全问题包括隐私和认证[1]。隐私问题主要包含信息泄露和位置追踪2个方面。信息泄露是指标签上储存的用户秘密信息被攻击者获知；位置追踪是指攻击者通过追踪标签获知持有该标签的人员或物品的位置信息。解决信息泄露的方法之一是将重要数据存储于得到完善安全保护的数据库上，而利用标签标识的Hash函数作为索引在数据库中查找对应的信息。解决位置追踪的2个条件为：不可分辨性和前向安全性[2]。不可分辨性意味着攻击者不能利用标签发送的信息将其与其他标签区分开来。前向安全性保证了即使攻击者获得了标签的数据信息，也不能回溯标签过去的行为。认证问题是指对标签合法性的确认，包括防止对标签克隆、伪造等。RFID系统受到计算能力、存储空间和电源供给等诸多因素的限制，难以实现复杂的安全算法。因此，设计安全、高效、低成本的RFID协议成为一个具有挑战性的课题，也吸引了众多研究者的关注。

2 相关研究

目前，RFID安全隐私保护方案可分为物理安全机制和基

基金项目：国家“863”计划基金资助项目“基于ISO18000-6 Type B/C标准的(UHF)标签芯片研发和产业化”(2006AA04A109)
作者简介：白 煜(1978－)，男，博士研究生，主研方向：信号与信息处理，射频识别技术；滕建辅、张立毅，教授、博士生导师；郭继昌，教授
收稿日期：2009-04-10 **E-mail：**baiyu220853@sina.com

于密码的安全机制。

基于物理的安全机制有法拉第网罩、“ Ki11 Tag ”杀死标签和“ Block Tag ”阻止标签等。

基于密码技术的 RFID 安全机制可以分为 2 大类：静态标识机制和动态标识刷新机制。静态标识机制就是标签的标识保持不变，如 Hash-Lock 协议[3]使用 metaID 代替真实的标签标识来避免信息泄漏和被追踪。而在动态标识刷新机制中，标签的标识随着每一次标签与读写器之间的认证交互而动态地变化，如 LCAP 协议[4]是一种问询-应答协议，标签每次完成对读写器的认证后都要动态刷新自身的标识。由于标签动态刷新标识，因此攻击者无法对标签进行跟踪。然而，采用动态标识刷新机制时，一个非常重要的问题就是“ 数据同步问题 ”[5]。数据同步是指数据库中所保存的标签标识必须和存储在标签中的标识同步刷新。否则，在下一次认证识别的过程中会出现合法标签无法通过读写器认证和识别的问题。此外，绝大多数低成本 RFID 标签都依靠外部环境的电磁感应供给能量，因此，标签很有可能会突然掉电。当这种情况发生时，RFID 安全协议应该仍然是健壮的。

文献[6]提出 Hash 链预计算协议(HPC)。HPC 协议使用变化的标签标识作为索引，要求数据库预测标签标识在 T 步内的变化值，并将这些标识全部作为数据库的索引，在合法交互后更新这些索引。当攻击者读取标签次数小于 T-1 次时，数据库可以采用索引查找找到标签标识；当攻击者读取标签次数大于 T-1 次而小于 T+M-1 次时(M 为 Hash 链的长度)，数据库可以采用 Hash 链查找找到标签标识。数据库保存最近一次交互的记录，即使发生标签掉电，当标签再次试图得到认证时仍然可以被识别。同时，HPC 协议实现了不可跟踪性和不可分辨性。但是，由于该协议基于 Hash 链，因此每一次标签认证发生时，后端数据库都要对每一个标签进行大量 Hash 运算，计算负担较大。同时，该协议需要 2 个不同的 Hash 函数，增加了标签的成本。

文献[7]提出一个轻量级 RFID 安全协议。该协议要求在标签与读写器互相认证之后，双方才更新所记录的标签标识。这样，可以防止攻击者破坏数据同步。但是，该协议并不能防止标签突然掉电造成的数据同步失败。

文献[8]提出 Key 值更新随机 Hash 锁安全协议。该协议使用了数据记录关联指针 pointer，能够保证数据同步性。关联指针 pointer 指导数据库增添、更新数据库记录后，数据库中会保存 2 条关于该标签的记录。当标签与读写器同步失败时，标签仍然可以使用未更新的标识与读写器进行互相认证。但是，该保护数据同步方法增加了数据库的查询时间。在每次询问过程中，设数据库中存储的标签个数为 N，该协议中后台数据库需执行 2N 个记录搜索。

由上述分析可知，如何保证数据库与标签的同步更新，是 RFID 安全协议的设计难点。本文针对这个问题提出了一种新的 RFID 安全协议。

3 基于 Hash 锁的同步强化 RFID 安全协议

本文综合已有协议的优点，提出基于 Hash 锁的同步强化 RFID 安全协议。该协议采用双向认证、动态密钥更新和数据同步加强等技术实现了防止信息泄露、位置跟踪和健壮性的安全要求。

3.1 协议工作原理

设数据库记录为 $[K,K_p,ID_k]$。其中，k 是数据库为每一个标签随机选取的密钥，存储于 K；K_p 是保护数据同步密钥；ID_k 为标签的唯一标识。$H(\cdot)$ 是单向 Hash 函数。标签记录的数据为 $[k,ID,data]$，其中，$data$ 为标签上存储的数据。

下面阐述该协议的基本工作原理：

(1)锁定标签

数据库选取一个随机数 k 作为标签的密钥，并将 k 发送给标签。建立该标签在数据库中的初始记录 $[K,K_p,ID_k]$，其中，K_p 为空，K 中存储值为 k。标签接收到密钥 k，存储之后进入锁定状态。假定上述过程是在安全的情况下完成。

(2)解锁标签

1)读写器发起请求：读写器生成随机数 R，将询问消息 $Query$ 和 R 都发送给标签。

2)标签应答：计算 $H(k\|R)$ 和 $H(ID\|R)$，将 $H(k\|R)$ 发送给读写器。

3)读写器认证标签：读写器通过安全信道将 $H(k\|R)$ 和 R 发送给数据库。数据库检查是否存在某个 k'，使得 $H(k'\|R)=H(k\|R)$ 成立。如果存在，则认证通过，协议进行下一步；否则忽略此消息，表明标签是非法标签。

4)数据库计算 $H(ID_k\|R)$，并将其与 ID_k 发送给读写器。读写器记录 ID_k，并将 $H(ID_k\|R)$ 发送给标签。

5)数据库更新记录：如果在步骤 3)中发现的 $k'\in K$，则将 k' 存储到 K_p，然后将 K 中存储的 k' 更新为 $H(k')$；如果 $k'\in K_p$，则不更新数据库。因为这意味着，读写器与标签之间发生数据同步失败，K 中存储着新的密钥，标签仍使用旧的密钥与读写器通信。

6)标签认证读写器：标签收到 $H(ID_k\|R)$ 后，与 $H(ID\|R)$ 进行比较，若相等则将自身 k 更新为 $H(k)$，标签进入解锁状态，对读写器开放其所有功能。若不相等，表明读写器为非法读写器，标签保持静默。

协议流程如图 2 所示。

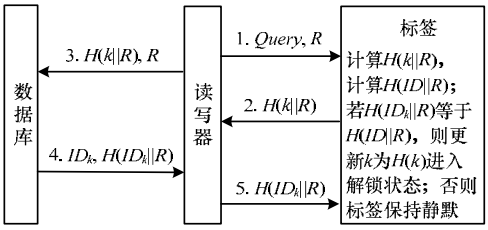

图 2　协议流程

3.2 安全性分析

本文提出的协议采用了密钥刷新机制。每次交互的数据在攻击者看来都具有随机性，攻击者即使获取了当前标签密钥值，也无法推算出之前的密钥值，所以无法获得标签相关的历史活动信息，即协议具有前向安全性；而且，由于 Hash 函数的单向性，攻击者无法确定 2 次交互的数据是否属于同一个标签，即协议具有不可分辨性。因此根据文献[2]，该协议实现了不可跟踪性。

标签只需要实现一个 Hash 函数，降低了标签的复杂性和成本。在每个验证过程中，标签和数据库分别只需要运行 3 次 Hash 函数和 1 次数值比较，与基于 Hash 链的安全协议相比，该协议运算负荷小、效率高。

对标签的重放攻击、哄骗攻击都无法通过协议中的标签验证。而且，非法修改标签数据的操作也会在读写器认证标

（下转第 143 页）