

A New RFID Secure Authentication Protocol Based on Hash

LI Hai-lin, XU Peng-fei

*Institute of Electronic Technology, Information Engineering University, Zhengzhou, 450004, China y
lihl_c@yahoo.com.cn*

Abstract: Being directed against the menace of security and privacy of RFID, a new Hash-based mutual authentication protocol for RFID security is proposed based on the analysis of some kinds of typical Hash-based protocols. The analysis shows that this novel protocol has the features of forward secure, low-load, high efficiency, good security and mutual authentication, and can prevent replay attack, wiretapping, counterfeit, spoof and location track.

Keywords: security protocol; Hash-based function; mutual authentication; RFID

一种基于 Hash 函数的 RFID 双向认证协议

李海林, 徐鹏飞

信息工程大学电子技术学院, 郑州, 中国, 450004
lihl_c@yahoo.com.cn

【摘要】针对 RFID 技术在安全隐私方面存在的威胁, 在分析了五种基于 Hash 的安全协议的特点和缺陷的基础上, 提出了一种新的基于 Hash 函数的双向 RFID 安全认证协议。分析表明, 该协议具有前向安全、效率高、安全性好、双向认证等特点, 能够有效防御重放攻击、窃听、仿冒、哄骗攻击和位置跟踪。

【关键词】安全协议; Hash 函数; 双向认证; RFID

1 引言

射频识别技术(Radio Frequency Identification, RFID)是一种非接触式的自动识别技术。它通过无线射频的方式读取和接收信息, 达到自动识别的目的。相比于条形码, 其使用方便、灵活, 所以应用极为广泛。目前, RFID 技术已被广泛用于零售、物流、生产、交通等各个行业。然而由于 RFID 系统自身存在的安全隐患, 同时在 RFID 系统的使用上也可能引发一系列隐私保护的问题, 因此研究如何更好地保证其安全性、隐私性至关重要。目前, 用基于密码技术设计的安全协议来实现对 RFID 系统的安全隐私保护比较流行, 而且成本也较低。但现有的种种安全协议都存在着不同程度的缺陷, 不能很好地实现对 RFID 系统的安全隐私保护。为此, 本文提出了一种新的基于 Hash 函数的 RFID 双向认证协议。

2 RFID 系统的组成及安全需求

2.1 RFID 系统的组成

RFID 系统组成如图 1 所示^[1]。RFID 系统一般由三

大部分组成: RFID 标签(Tag)、RFID 读写器(Reader)、后端数据库(Database)。RFID 标签是配备有天线的微型电路, 通常没有微处理器, 仅由数千个逻辑门电路组成。读写器实际是一个带有天线的无线发射与接收设备, 它的处理能力、存储空间都比较大。后端数据库可以是运行于任意硬件平台的数据库系统, 它包含所有 Tag 的信息。

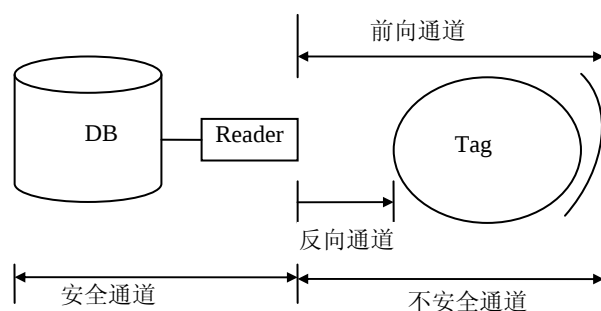


图 1 RFID 系统组成

2.2 RFID 系统的安全需求

为确保安全隐私, RFID 系统需满足如下安全需求:

1) 可追踪性

部署和使用 RFID 系统时, 关键的问题之一是要确保只有授权用户能够识别各个标签(Tag), 而攻击者无法对这些标签进行任何形式的跟踪。

2) 重放攻击

在读写器发出认证请求时, 攻击者可能偷听获取到标签的响应。在下一轮的认证过程中, 攻击者发送已获得的数据至读写器, 从而通过认证。因此, RFID 系统必须具有应对重放攻击的能力。

3) 哄骗攻击

攻击者伪装为合法读写器, 发送认证请求, 进而获得标签响应输出。当合法读写器询问标签时, 攻击者将获得标签响应发送给读写器。这样攻击者屏蔽了真实标签的响应, 通过了读写器的认证。

4) 通信量分析

对读写器和标签的信息截取、分析, 提取有用信息的过程。攻击者向标签发送多次的询问请求, 接收标签返回数据。从获得的数据中分析标签的响应, 达到跟踪标签的目的。

3 RFID 安全协议相关研究

目前基于 Hash 函数的 RFID 安全协议较多, 下面对其进行简单分析。

3.1 Hash-Lock 协议

Hash-Lock 协议^[2,3]是由 Sarma 等人提出的, 为了避免信息泄漏和被追踪, 它使用 metaID 来替代真实的标签 ID。其协议流程如图 2 所示。

可以看出, 协议中的信息都是以明文的形式进行传送, 没有 ID 动态刷新机制, 因此该协议非常容易被窃听和假冒, 攻击者也可以很容易地对标签进行位置跟踪。

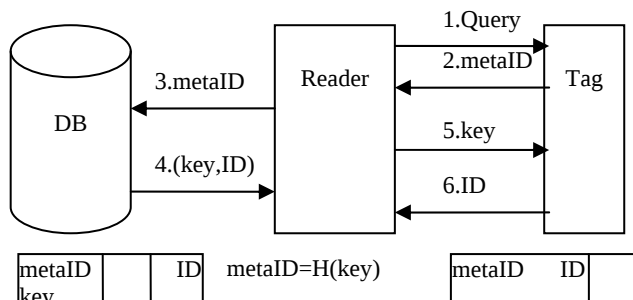


图 2 Hash-Lock 协议

3.2 随机 Hash-Lock 协议

随机 Hash-Lock 协议^[4]由 Weis 等人设计, 它针对 Hash-Lock 协议传输明文信息的缺点进行改进, 采用了基于随机数的询问-应答机制, 其协议流程如图 3 所示。

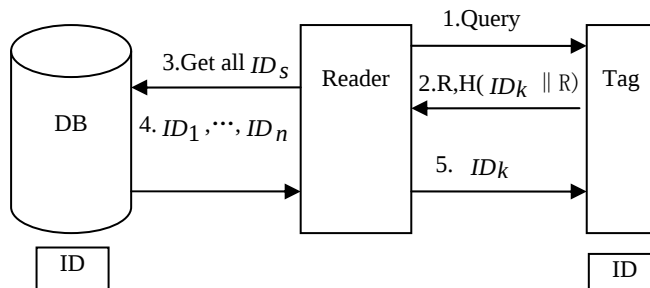


图 3 随机 Hash-Lock 协议

在该协议中, 认证通过后的 ID 仍以明文的形式传送, 因此攻击者可以对标签实施位置跟踪。同时, 该协议也无法抵挡假冒和重放攻击。而且随机数由标签生成, 增加了标签的成本。

3.3 Hash 链协议

Hash 链协议也是基于共享秘密的询问-应答协议^[5]。但是, 在 Hash 链协议中, 当使用两个不同杂凑函数的 Tag 读写器发起认证时, Tag 总是发送不同的应答, 其协议流程如图 4 所示。

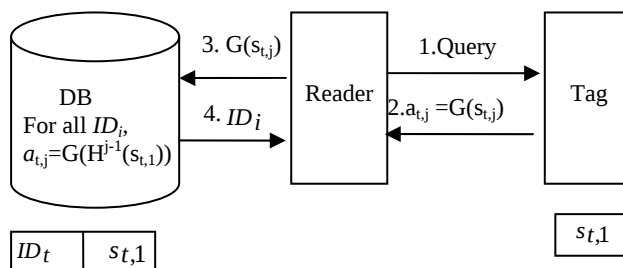


图 4 Hash 链协议

该协议利用标签每次更新标识满足了不可分辨性和前向安全性。然而, Hash 链协议是一个单向认证协议, 它只对标签进行认证, 容易受到重放和哄骗攻击。此外, 在每次认证过程中, 后端数据库都要对每一个 Tag 进行 J 次杂凑运算, 因此其计算载荷也很大。同时, 该协议需要两个不同的杂凑函数, 也增加了 Tag 的制造成本。

3.4 LCAP 协议

LCAP 协议基于询问-应答机制的协议^[6], 与其它协议不同, 它每次执行后都要更新标签的标识 ID。其协议流程如图 5 所示。

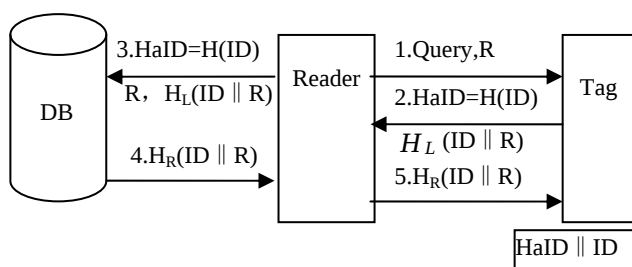


图 5 LCAP 协议

在协议中，标签是在接收到消息 5 且验证通过之后才更新 ID 的，而在此之前，后端数据库已经成功完成 ID 的更新。因此，存在着数据库与标签中信息的同步问题。

3.5 一种改进后的 Reader-Tag 通信协议

该协议由武汉数字工程研究所的陈雁飞等人提出，后端数据库记录主要包括 $H(\text{Key})$, ID, Key 和 Pointer, 主键为 $H(\text{Key})$ ^[7]。其中 ID 为标签唯一标志号，Key 是读写器为每个标签选取的随机关键字， $H(\text{Key})$ 是 Key 的单向 Hash 函数 H 计算值，Pointer 是数据记录关联指针，主要用来保证数据的一致性。协议流程如图 6 所示。

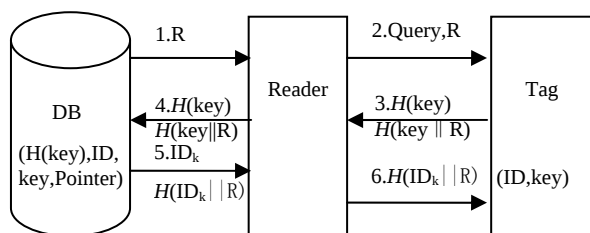


图 6 Reader—Tag 通信协议

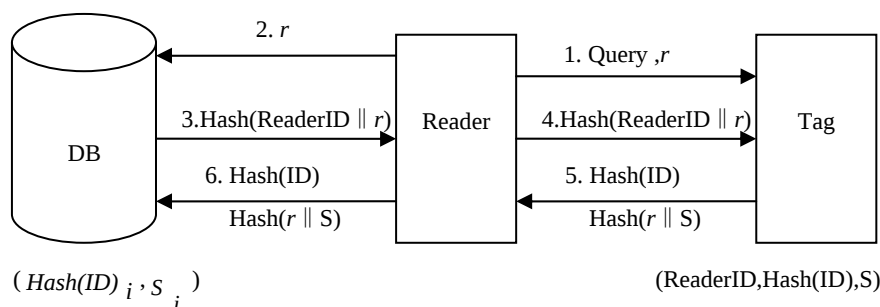


图 7 基于 Hash 函数的双向认证协议

认证步骤如下：

- 1) 读写器向标签 Tag 发送认证请求，同时产生随机数 r ，并将 r 发送给标签；
- 2) 读写器将 r 发送给后端数据库；
- 3) 后端数据库根据存储的读写器的标识 ReaderID 和随机数 r ，计算 $\text{Hash}(\text{ReaderID} \parallel r)$ ，将 $\text{Hash}(\text{ReaderID} \parallel r)$ 发送给读写器；
- 4) 读写器将 $\text{Hash}(\text{ReaderID} \parallel r)$ 转发给标签；

该协议具有成本较低、安全性较高的特点，但还存在一些不足，如，尚无法防止敌人根据流量分析(计算标签的个数)而进行的定位跟踪，同时安全性提高也增加了标签部分计算时延，并且还存在着与国际相关标准兼容性的问题。

4 一种基于 Hash 函数的双向认证协议

本文提出的协议同样采用了询问—应答机制。它通过实现标签与读写器之间的双向认证，能够有效地防御重放攻击、窃听和哄骗攻击。同时，由于采用了对读写器进行标识，能够防御位置跟踪。

4.1 工作原理

4.1.1 初始条件

1) 标签(Tag): 在标签中存储 $(\text{ReaderID}, \text{Hash}(\text{ID}), S)$ 。其中 ReaderID 是读写器的标识， $\text{Hash}(\text{ID})$ 是标签 ID 的 Hash 值， S 是秘密信息。

2) 读写器(Reader): 为每个读写器配置一个固定的标识 ReaderID。在实际应用时，可以为一批读写器配置相同的标识。

3) 后端数据库(Database): 存储有读写器的标识 ReaderID，同时还存储了每个标签的 $\text{Hash}(\text{ID})$ 与秘密信息 S 的对应组 $(\text{Hash}(\text{ID})_i, S_i)$ 。

4.1.2 认证过程

协议认证过程如图 7 所示：

- 5) 标签根据自身存储的 ReaderID 和接收到的 r ，计算 $\text{Hash}(\text{ReaderID} \parallel r)$ ，并与接收到的 $\text{Hash}(\text{ReaderID} \parallel r)$ 相比较。若相等，则标签对读写器认证通过，标签计算 $\text{Hash}(r \parallel S)$ ，将 $\text{Hash}(\text{ID})$ 与 $\text{Hash}(r \parallel S)$ 一起发送给读写器；否则认证失败。

- 6) 读写器将 $\text{Hash}(r \parallel S)$ 与 $\text{Hash}(\text{ID})$ 转发给后端数据库；

7) 后端数据库根据 $\text{Hash}(\text{ID})$ 查找秘密信息 S_i , 计算 $\text{Hash}(r \parallel S_i)$, 并与 $\text{Hash}(r \parallel S)$ 相比较, 若相等, 则读写器对标签认证通过, 开始传送数据; 否则认证失败。

在协议中, 因为标签需要进行两次 Hash 计算, 所以要采用主动型标签。同时, 标签内部也需要有值比较电路。标签内部具体的流程如图 8 所示。

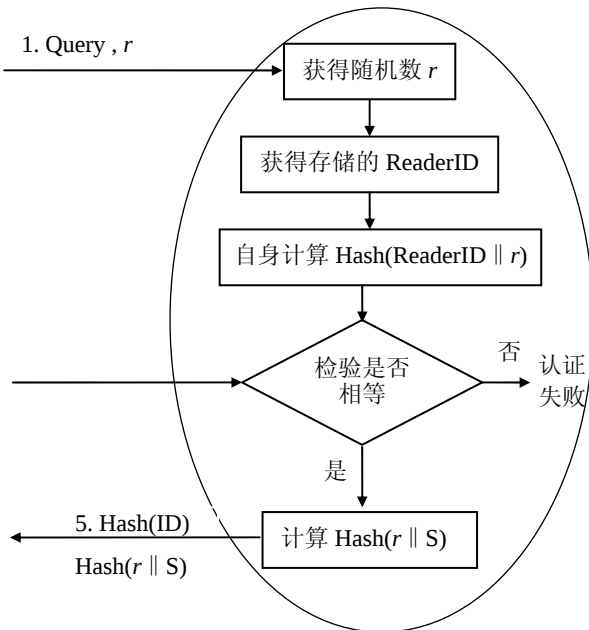


图 8 标签内部流程

4.2 性能分析

1) 简单实用。由读写器产生随机数, 降低了标签的复杂性。在一次认证中, 标签只需要实现两次 Hash 运算和一次值比较, 这在低成本标签上较易实现。

2) 防止伪造标签。即使攻击者非法窃听了标签的所有输出, 由于 r 是随机产生的, 所以在步骤 (7) 中读写器也能够识别出标签的真伪。

3) 防止伪装读写器。由于采用了对读写器进行标识, 即使攻击者伪装读写器, 他也无法通过步骤 (5) 中标签对读写器的检验。

4) 防止位置跟踪。标签对非法读写器是屏蔽的, 只对被认证的读写器响应。根据协议, 攻击者伪装读写器时, 无法获得任何标签的输出。所以, 攻击者无法对标签进行位置跟踪。

5) 实现身份的双向认证。通过步骤 (5), 标签实现了对读写器的认证。通过步骤 (7), 读写器实现了对标签的认证。

6) 低计算负载。在一次认证中, 后端数据库要进行两次 Hash 运算、一次值比较和 N 个记录搜索。相比于 Hash 链协议, 计算负载显著降低。

5 结束语

RFID 技术在 21 世纪有着广阔的发展前景, 所以如何更好地保证 RFID 系统的安全性, 是一项重要的研究课题。用密码技术来解决安全问题是比较可靠的方法。本文提出的基于 Hash 函数的双向认证协议具有高安全性、低成本等优点, 能够有效地防御重放攻击、窃听、哄骗攻击和位置跟踪, 具有较高的实用价值。

References (参考文献)

- [1] 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.
ZHOU Yong-Bin, FENG Deng-Guo. Design and Analysis of Cryptographic Protocols for RFID[J]. Chinese Journal of Computers. 2006. 29 (4): 581-589.
- [2] Sarma S. E, Weis S. A, Engels D. W. RFID systems and security and privacy implications[C]. In: Kaliski B. S., Koc C. K., Paar C. eds. Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2002), Lectures Notes in Computer Science 2523. Berlin: Springer-Verlag, 2003: 454-469.
- [3] Sarma S. E., Weis S. A., Engels D. W. Radio-frequency identification Secure risks and challenges[J]. RSA Laboratories Cryptobytes, 2003,6(1): 2-9.
- [4] Weis S. A., Sarma S. E., Rivest R. L., et al. Security and privacy aspects of low-cost radio frequency identification systems. In: Hutter D., Stephan W., Ullmann M. eds. Proceedings of the 1st International Conference on Security in Pervasive Computing. Lectures Notes in Computer Science 2802, Berlin: Springer-Verlag, 2004: 201-212.
- [5] Ohkubo M., Suzuki K., Kinoshita S. Hash-chain based forward-secure privacy protection scheme for low-cost RFID [C]. In: Proceedings of the 2004 Symposium on Cryptography and Information Security (SCIS 2004), Sendai, 2004: 719-724.
- [6] Lee S. M., Hwang Y. J., Lee D. H. Efficient Authentication For Low-cost RFID Systems. Proceedings of the International Conference on Computational Science and Its Applications. LNCS 3480.2005: 619-627.
- [7] 陈雁飞, 马成勇, 杨慧. 基于 RFID 系统的 Reader-Tag 安全协议的设计及分析[J]. 计算机与数字工程, 2008, 36 (9), 128-131.
- [8] Chen Yanfei, Ma Chengyong, Yang Hui. Design and Analysis of Security Protocol for Reader-Tag Based on RFID System [J]. Computer & Digital Engineering. 2008, 36 (9):128-131.