

# 基于 Hash 函数的移动射频识别互认证安全协议设计

刘 鹏\*, 张昌宏, 欧庆于

(海军工程大学 信息安全系, 武汉 430033)

(\* 通信作者电子邮箱 taisui808@163.com)

**摘 要:**为解决移动射频识别(RFID)中阅读器与后端服务器分离所产生的安全问题,设计出一种基于 Hash 的轻量级认证协议,在无线通信环境下利用 Hash 的单向性实现标签、阅读器和后端服务器之间三方的互相认证,防止重放攻击、非法读取、位置跟踪等一系列安全问题的发生;并将计算的主要成本转移到后端服务器,减小大规模应用标签的开支。对协议进行 GNY 逻辑推理,证明其安全性足够满足应用的要求。

**关键词:**移动 RFID;互认证;Hash 函数;形式化分析;轻量级;GNY 逻辑

**中图分类号:** TP393.04 **文献标志码:** A

## Authentication protocol of mobile RFID based on Hash function

LIU Peng\*, ZHANG Changhong, OU Qingyu

(Department of Information Security, Naval University of Engineering, Wuhan Hubei 430033, China)

**Abstract:** In order to resolve the security issues of Mobile-Radio Frequency Identification (M-RFID), the author designed a lightweight authentication protocol based on Hash. It can achieve the mutual authentication between tags, readers and servers in the environment of wireless communication. It can prevent a series of security issues such as replay attacks, unauthorized reading, and location tracking. GNY logic was applied to prove that the agreement is sufficient to meet the security needs.

**Key words:** mobile RFID; mutual authentication; Hash function; formal analysis; lightweight; GNY logic

## 0 引言

射频识别(Radio Frequency Identification, RFID)是比较常用的一种自动识别技术,不需要直接接触就可以对信息载体内的有效数据进行读写,目前被广泛地用于物流、防伪、门禁、生产管理等领域。由于使用无线通信技术,暴露的通信信道不可避免地存在安全隐患。针对这些问题,国内外学者设计出多种安全认证协议。如 Weis<sup>[1]</sup>提出的 hash-lock,身份符号(Identity, ID)是明文传送的,不能防止跟踪,ID 的变换形式 metalID 是一直不变的,不能防止重放攻击和假冒。Weis 等<sup>[2]</sup>提出的随机 hash-lock 协议在 hash-lock 的基础之上增加了随机数  $R$ ,可以有效地防止重放攻击,但是在最后阶段阅读器仍然用明文传送标签的 ID 进行验证,不可避免地产生被跟踪的威胁,而且每次申请都要求服务器发送所有 ID 给阅读器,增加了通信量。日本电报电话公共公司网络创新实验室(Nippon Telegraph and Telephone Public Corporation Network Innovation Laboratories, NTT)提出的 Hash-chain 协议<sup>[3-4]</sup>,能够实现密钥的更新,但是不能实现对标签的认证。同时这些协议没有考虑移动射频识别(Mobile Radio Frequency Identification, M-RFID)中阅读器与后端服务器无线通信的特性。国内的大部分研究者在讨论移动 RFID 的认证问题时也都假定阅读器与后端服务器之间的无线通信是可靠的,这对于暴露的无线信道来说显然不合理。如文献[5]中的协议不能防止对标签的重放攻击,在文献[6-7]中阅读器没有对服务器进行认证,这样的认证协议都不适用于 M-RFID。

针对这些协议的不足,利用 Hash 函数的单向性设计了一种能解决 M-RFID 安全问题的互认证协议,使标签、阅读器与

后端的服务器三方进行相互的认证,经 GNY 逻辑证明了其安全性<sup>[8]</sup>。

## 1 RFID 原理

### 1.1 RFID 构成

射频识别系统由三部分组成:标签、阅读器和服务器。标签中存储产品的信息;阅读器对标签中的内容进行读写;服务器处理阅读器发送过来的数据并保存整个 RFID 系统的各种信息(如标签 ID、通信密钥、会话应答号等)。通常情况下,阅读器通过发射电磁信号为标签提供能量,标签经无线信道向阅读器发送产品的相关信息,阅读器再将接收到的数据传送给后方的服务器进行处理<sup>[9]</sup>。但是,随着无线通信技术、智能终端(如手机、平板电脑)的不断发展使手持阅读器更加智能,使用更加方便,传统的 RFID 系统即将被 M-RFID 所取代。M-RFID 系统的阅读器断开了与后端服务器的有线连接,被嵌在可移动的智能终端内部,从服务器接收到的产品信息更加直接快速地反映到用户面前。其结构如图 1 所示。

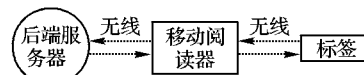


图 1 移动 RFID 系统结构

### 1.2 移动 RFID 的安全隐患<sup>[5-6]</sup>

移动 RFID 与传统射频识别系统的主要区别在于其阅读器与后端服务器是无线连接的,使阅读器的应用更加灵活,为用户提供更加方便快捷的服务。在方便的同时带来了新的问题,总结起来其主要安全隐患如下:

1) 位置跟踪。标签泄露自己唯一的 ID,攻击者在用户不知情的情况下通过标签的响应来实现非法跟踪。

收稿日期:2012-11-27;修回日期:2012-12-29。

**作者简介:**刘鹏(1988-),男,河北衡水人,硕士研究生,主要研究方向:密码理论、密码保障;张昌宏(1964-),男,江苏扬州人,副教授,硕士,主要研究方向:密码保障;欧庆于(1978-),男,江西靖安人,副教授,硕士,主要研究方向:密码芯片设计。

2) 重放攻击。攻击者截获合法设备发送的信息,在未授权的情况下重复发送给特定的设备(如标签、阅读器、服务器)来骗取相应的服务或数据。

3) 窃听威胁。设备之间经暴露的无线信道,用明文进行数据传输,很容易被未授权的第三方截获,从而进行窃听行为。

4) 伪造。攻击者通过伪造通信实体对系统进行攻击。这在移动 RFID 系统中尤为突出。可以对服务器进行伪造来骗取标签与阅读器的 ID、内存等信息;对阅读器进行伪造以欺骗服务器,实现套取标签数据的目的;对标签进行伪造从而达到欺骗用户的目的。

5) 非法访问。在未授权的情况下对设备中的数据数据进行读写,导致合法的数据失去利用价值。

## 2 基于 Hash 函数的移动 RFID 认证协议

针对 M-RFID 的安全需求,设计了一种基于 Hash 函数的互认证协议,能够有效地避免以往安全协议的漏洞,满足 M-RFID 的移动特性;并且最大限度地减小了标签和阅读器的计算量,节约成本。具体的协议流程如图 2 所示。

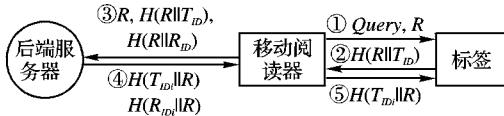


图2 认证协议流程

图2中, $R$ 表示阅读器产生的随机数, $H()$ 表示对数据进行 Hash 计算,“||”表示字符连接符号, $T_{id}$ 表示标签唯一的 ID, $R_{id}$ 表示阅读器唯一的 ID。后端服务器中存有所有阅读器与标签的 ID。

认证协议工作原理:

1) 阅读器向标签发送询问申请 *Query*,同时将自己产生的随机数  $R$  发送至标签。每次产生的随机数不相同,也不能由以前的随机数推导出后续的  $R$ 。

2) 标签接收到阅读器的申请后计算  $H(R||T_{id})$  与  $H(T_{id}||R)$ ,并将  $H(R||T_{id})$  发送至阅读器,同时将  $H(T_{id}||R)$  保存在标签内存中。

3) 阅读器计算  $H(R_{id}||R)$  与  $H(R||R_{id})$ ,将  $R$ 、 $H(R||R_{id})$ 、 $H(R||T_{id})$  发送至后端的服务器,在阅读器内存中保存  $H(R_{id}||R)$ 。

4) 后端的服务器计算在数据库中是否存在相应的  $R_{id}$ ,使得  $H(R||R_{id}) = H(R||R_{id})$ ,如果存在,则阅读器通过认证;服务器继续在数据库中查找是否有相应的  $T_{id}$  使得  $H(R||T_{id}) = H(R||T_{id})$ ,如果存在,则标签通过服务器的认证。当两者都通过认证后,服务器计算  $H(T_{id}||R)$  与  $H(R_{id}||R)$  并发送至阅读器。

5) 阅读器核对收到的  $H(R_{id}||R)$  与自己内存中的  $H(R_{id}||R)$  是否相等,如果相等则服务器通过阅读器的认证。阅读器收到正确的  $H(R_{id}||R)$  则表示得到服务器的保证,证明标签是合法的。阅读器将接收到的  $H(T_{id}||R)$  发送至标签。

6) 标签接收到阅读器的信息后,核对与自己内存中的  $H(T_{id}||R)$  是否相等,如果相等,则阅读器与服务器通过标签的认证。

## 3 性能分析

设计的基于 Hash 的认证协议具有如下优点:

1) 抗重放。阅读器每次申请通信都生成不同的随机数  $R$ ,该随机数贯穿整个认证过程,即使攻击者截获某次通信的数据也不能在以后的通信中对系统进行重放攻击<sup>[10]</sup>。

2) 防跟踪。在通信过程中阅读器与标签的 ID 始终是以与随机数  $R$  进行 Hash 后的形式进行传输的,即使攻击者截获了数据也不能推断出真实的 ID,从而不能完成对特定标签的追踪。

3) 防窃听。在无线信道中传输的数据都是没有实际意义的随机数或者 Hash 值,对于攻击者来说没有任何利用价值,不涉及对通信内容的窃听<sup>[11]</sup>。

4) 抗伪造。该协议最大的优点是实现了 M-RFID 系统的认证,使标签、阅读器、服务器进行了相互认证,任何一个实体的伪造都不能通过认证协议的严密审核,完全避免了文献[2-4]中存在的安全漏洞。

5) 采用 Hash 这种计算量较小的方式,大大节省了应用的成本<sup>[12]</sup>。

通过以上的性能分析可以看出本协议具有很好的适应性,完全能够解决 M-RFID 系统面临的各种安全问题,而且将计算的成本转移到了后台服务器,比较适合大规模的应用。

## 4 GNY 逻辑形式化分析

GNY 逻辑<sup>[8]</sup>是目前影响最大的一种形式化分析工具,形式化的分析能够让研究者发现安全协议的安全漏洞,这是从主观上简单推理所不能达到的。现在用 GNY 逻辑对协议的安全性进行论证。

标签用  $T$  表示,阅读器用  $R_e$  表示,服务器用  $S$  表示,Hash 算法用  $H_k$  表示。

证明思路: $S$  接收到  $R_e$  的信息后完成对  $R_e$  与  $T$  的认证; $R_e$  接收到  $S$  的回复后完成对  $S$  的认证; $R_e$  转发  $S$  的信息,完成  $T$  对  $R_e$  的认证。全程有随机数  $R$  参与,保证新鲜性。

部分 GNY 规则:

被告知规则 (Being-Told Rules):

$$\frac{P \triangleleft * X \quad P \triangleleft (X, Y) \quad P \triangleleft \{X\}_K, P \ni K}{P \triangleleft X, \quad P \triangleleft Y, \quad P \triangleleft X}$$

新鲜性规则 (Freshness Rules):

$$\frac{P \models \#(X)}{P \models \#(X, Y), \quad P \models \#(F(X))}$$

识别性规则 (Recognizability Rules):

$$\frac{P \models \varphi(X), \quad P \ni X \quad P \ni H(X)}{P \models \varphi(H(X)), \quad P \models \varphi(X)}$$

消息解释规则 (Message Interpretation Rules):

$$\frac{P \triangleleft * \{X\}_K, \quad P \ni K, \quad P \models P \triangleleft Q, \quad P \models \varphi(X), \quad P \models \#(X, K)}{P \models Q \sim X, \quad P \models Q \sim \{X\}_K, \quad P \models Q \ni K}$$

1) 对消息进行形式化转换,确立要证明的目标,对已知的信息进行假设。

消息转换:

M1:  $T \triangleleft R$

M2:  $R_e \triangleleft H(R||T_{id})$

M3:  $S \triangleleft * R, H(R||T_{id}), H(R||R_{id})$

M4:  $R_e \triangleleft H(R_{id}||R), H(T_{id}||R)$

M5:  $T \triangleleft H(T_{id}||R)$

证明目标:

O1:  $S \models R_e \sim \#R, \#H(R||R_{id})$  服务器认证阅读器;

O2:  $R_e \models S \sim \#H(R_{id}||R)$  阅读器认证服务器;

O3:  $T \models R_e \sim \#H(T_{id}||R)$  标签认证阅读器。

假设条件:

A1:  $T \ni T_{id}$ ;

A2:  $R_e \ni R_{id}, H_k$ ;

A3:  $S \ni R_{id}, T_{id}, H_k$ ;

A4:  $R_e \ni R$ ;

$A5: R_e \models \varphi(R_{ID} \parallel R);$

$A6: T \models \varphi(T_{ID} \parallel R);$

$A7: S \models \varphi(R \parallel R_{ID}), \varphi(R \parallel T_{ID}).$

2) GNY 逻辑证明。

①  $S \models R, S \models H(R \parallel R_{ID}), S \models \#R$  (由 M3 得);

②  $S \models \#(R \parallel R_{ID} \parallel H_k), S \models \#H(R \parallel R_{ID})$  (由 ① 新鲜性规则得);

③  $S \models \#R_e \sim H(R \parallel R_{ID})$  (由 A2、A3、A7、② 消息解释规则得);

④  $S \models R_e \sim \#R, \#H(R \parallel R_{ID})$  (由 ②、③ 得)。

至此 O1 完成。

本协议最重要的就是服务器对阅读器与标签的认证,服务器整个认证过程的中介。同理多次利用新鲜性规则与消息解释规则,结合已知条件可以得到下式:

$O2: R_e \models S \sim \#H(R_{ID} \parallel R)$

$O3: T \models R_e \sim \#H(T_{ID} \parallel R)$

至此完成协议的安全性认证,三方都得到了有效的相互认证,证明该协议符合实际应用的条件。

## 5 结语

针对现有 RFID 认证协议在安全性与适应环境方面的不足,本文提出了一种基于 Hash 的轻量级认证协议,该协议可以有效防止重放、位置跟踪、伪造等一系列攻击,并适应了移动射频识别系统中阅读器与后端服务器无线通信的环境,同时服务器承担了大部分相对复杂的计算,将成本转移至后端的服务器,有助于大规模应用的实现。并经 GNY 逻辑形式化的推理,证明该协议在逻辑上不存在漏洞,可以满足移动 RFID 系统中三方通信实体身份认证的需求。

### 参考文献:

(上接第 1349 页)

$$U_d = \begin{matrix} & s_d^1 & s_d^2 & s_d^3 & s_d^4 & s_d^5 \\ \begin{matrix} s_a^1 \\ s_a^2 \\ s_a^3 \end{matrix} & \begin{bmatrix} 161.28 & 120.96 & 147.84 & 174.72 & 137.40 \\ 136.32 & 151.68 & 109.44 & 141.12 & 151.68 \\ 174.72 & 107.52 & 117.60 & 117.60 & 137.76 \end{bmatrix} \end{matrix}$$

根据纳什均衡的存在条件<sup>[13]</sup>:任意有限策略型博弈至少存在一个混合策略纳什均衡。由最优策略选取算法可得最优混合策略均衡解  $S_a = (0.243, 0.645, 0.111)$ ,  $S_d = (0.217, 0, 0, 0.068, 0.715)$ 。由此可见,攻击者为了达到攻击目标,最可能以 0.243 的概率采取攻击策略  $s_a^2$ ,而防御者为了达到最佳防御效果则应主动采取策略  $s_d^5$  进行防御。

## 5 结语

本文针对网络安全问题具有利益对立性、策略依存性的特点结合博弈论提出了一种网络安全博弈图。在此基础上,结合实际攻防环境将网络攻防对抗理解为两人非合作、非零和博弈模型,从网络安全属性的角度给出了攻防成本量化方法。实验结果表明,本文所提出的评估模型能有效对攻击行为做出预测,并为系统做好主动防御提供最优防御策略选择。

### 参考文献:

- [1] 林闯,汪洋,李泉林. 网络安全的随机模型方法与评价技术[J]. 计算机学报, 2005, 28(12): 1943-1956.
- [2] BROWNE R. C4I defensive infrastructure for survivability against multi-mode attack[C]// Proceedings of the 21st Century Military Communication - Architectures and Technologies for Information Su-

- [1] WEIS S A. Security and privacy in radio-frequency identification devices [D]. Cambridge: Massachusetts Institute of Technology, Department of Electrical Engineering and Computer Science, 2003.
- [2] WEIS S, SARMA S, RIVEST R, *et al.* Security and privacy aspects of low-cost radio frequency identification systems[C]// Proceedings of Security in Pervasive Computing'04. Piscataway: IEEE Computer Society Press, 2004: 201-212.
- [3] 曾丽华,熊璋,张挺. Key 值更新随机 Hash 锁对 RFID 安全隐私的加强[J]. 计算机工程, 2007, 33(3): 151-155.
- [4] OHKUBO M, SUZUKI K, KINOSHITA S. Cryptographic approach to "Privacy-Friendly" tags[C]// Proceedings of RFID Privacy Workshop. Cambridge: Massachusetts Institute of Technology Press, 2003: 212-219.
- [5] 陈信刚. 基于移动网的 RFID 安全接入机制研究[D]. 南京: 南京邮电大学, 2008.
- [6] 王新锋,刘建国,蒋旭,等. 移动型 RFID 安全协议及其 GNY 逻辑分析[J]. 计算机应用, 2008, 28(9): 2239-2241.
- [7] 张亚玲,张超奇,马巧梅. 读写器可移动的 RFID 高效认证协议[J]. 计算机工程, 2012, 38(1): 264-267.
- [8] GONG L, NEEDHAM R, YAHALOM R. Reasoning about belief in cryptographic protocols[C]// Proceedings of the 1990 IEEE Computer Society Symposium on Research in Security and Privacy. Washington, DC: IEEE Computer Society, 1990: 234-248.
- [9] 米志强. 射频识别(RFID)技术与应用[M]. 北京: 电子工业出版社, 2011.
- [10] 马巧梅,王尚平. 一个超轻量级的 RFID 认证协议[J]. 计算机工程, 2012, 38(2): 151-153.
- [11] 邓森磊,王玉磊. 无需后端数据库的 RFID 认证协议[J]. 北京邮电大学学报, 2009, 32(4): 59-62.
- [12] 蔡豪. RFID 安全认证协议的研究与设计[D]. 武汉: 华中科技大学, 2010.
- [13] LEE E, WONG J. The theory of games with applications. Washington, DC: IEEE Computer Society, 2000, 1: 417-424.
- [3] 林旺群,王慧,刘家红,等. 基于非合作动态博弈的网络安全主动防御技术研究[J]. 计算机研究与发展, 2011, 48(2): 306-316.
- [4] 张少俊,李建华,陈秀真,等. 基于动态博弈理论的分布式拒绝服务攻击防御方法[J]. 上海交通大学学报, 2008, 42(2): 198-201.
- [5] LYE K, WING J M. Game strategies in network security[J]. International Journal of Information Security, 2005, 4(1): 71-86.
- [6] 曹晖,王青青,马义忠,等. 基于动态贝叶斯博弈的攻击预测模型[J]. 计算机应用, 2007, 27(6): 1545-1547.
- [7] 王纯子,黄光球. 基于粗糙贝叶斯博弈的网络攻防策略[J]. 计算机应用, 2011, 31(3): 784-789.
- [8] HADI O, MONA M, CHADI A, *et al.* Game theoretic models for detecting network intrusions[J]. Computer Communications, 2008, 31(10): 1934-1944.
- [9] SALLHAMMAR K, HELVIK B E, KNAPSOG S J. On stochastic modeling for integrated security and dependability evaluation[J]. Journal of Networks, 2006, 1(5): 31-42.
- [10] 王元卓,林闯,程学旗,等. 基于随机博弈模型的网络攻防量化分析方法[J]. 计算机学报, 2010, 33(9): 1748-1762.
- [11] 司加全,张冰,荷大鹏,等. 基于攻击图的网络安全性增强策略制定方法[J]. 通信学报, 2009, 30(2): 123-128.
- [12] ROBERT G. A primer in game theory[M]. Princeton: Princeton University Press, 1992.
- [13] OSBORNE M J, RUBINSTEIN A, AUMANN R, *et al.* A course in game theory [M]. 2nd ed. Cambridge: MIT Press, 1994.