RFID认证协议的安全性分析

王明辉[1,2],郑 周[2],唐拥政[1,2]
(1.盐城工学院 信息工程学院,江苏 盐城 224051; 2.盐城工学院 现代教育技术中心,江苏 盐城 224051)

摘要:针对RFID认证协议本身的安全性问题,分析了最近提出的几个协议的优缺点,给出了它们在一些安全特性上的比较,结果表明它们在某些方面都存在一些安全漏洞。通过对协议研究和分析,表明目前提出某些认证协议没有达到RFID系统的安全需求。只有通过更加有效的方法,才能设计出完全可靠、安全和高效的安全协议。

关键词:射频识别;认证;隐私;安全协议
中图分类号:TP311.563 **文献标识码**:A **文章编号**:1671-5322(2012)01-0045-04

射频识别技术(radio frequency identification)简称为RFID技术,它是最近几年来兴起的新技术。由于RFID标签本身具有体积小、有一定存储能力、寿命长、可重复使用等特点,并且,它利用无线射频方式进行通信,能够达到捕捉高速移动物体并对其快速读写、快速移动识别、多目标识别、定位及跟踪等。目前,射频识别技术已被广泛应用于交通管理、仓储管理、供应链管理、物流管路、流水线生产自动化、校园一卡通管理和汽车防盗等领域。随着电子标签成本的越来越低和新材料的不断出现,RFID的应用前景将更广阔。

随着RFID应用的推广,RFID系统的安全性也越来越受到人们的关注。由于读写器与电子标签之间采用的是无线射频通道进行传输,因此在便利的同时也给通信本身的安全性带来一定的威胁(例如,用户的隐私泄漏,用户被跟踪等)。为了解决此类安全问题,研究者们提出了多个解决方案。其中一些学者采用Hash函数技术,提出了很多的认证协议[1-3],而Hash函数的计算量大,对标签的要求很高。为了让它能够在轻量级的、低端的标签中使用,EPC Global组织制定了EPC Class 1 Gen 2 (EPCGen2)标准[4]。标准中提出在RFID认证协议中只能利用一个16bit的伪随机数生成器(PRNG)和一个16bit的循环冗余校验码(CRC),可以进行基于简单的异或(XOR)操作和矩阵操作,不能采用加密函数和Hash函数。随后,研究者提出了一些符合EPCGen2标准的RFID认证协议[5-7]。本文对这两类的RFID认证协议进行了安全性分析,指出了最近提出的一些协议同样存在安全缺陷,并给出了它们在某些安全属性上的对比结果。

1 RFID系统研究

1.1 RFID系统的组成

RFID技术凭借感应电流所获得的能量发送出存储在芯片中的产品信息(Passive Tag,无源标签或被动标签),或者由标签主动发送某一频率的信号(Active Tag,有源标签或主动标签),解读器读取信息并解码后,送至中央信息系统进行有关数据处理。一个完整的RFID系统一般由3个主要部件组成:RFID标签(tag)、RFID读写器(Reader)和后端数据库(DB Server),如图1所示。从RFID读写器到标签的信道,称为前向信道(forward channel),通过无线射频的方式读取和接收信息,是不安全信道;标签到读写器的信道,称之为后向信道(backward channel),信号强度相对较弱,也是不安全信道。后端数据库和读卡器之间是安全信道,数据库接收来自RFID读写器的数据,通过检索和标签相关的数据对标签进行实体认证。

1.2 RFID的安全需求

为确保消费者的消费安全,促进RFID得到

收稿日期:2011-02-21
作者简介:王明辉(1977-),男,黑龙江绥棱人,讲师,硕士,主要研究方向为信息安全与密码协议。

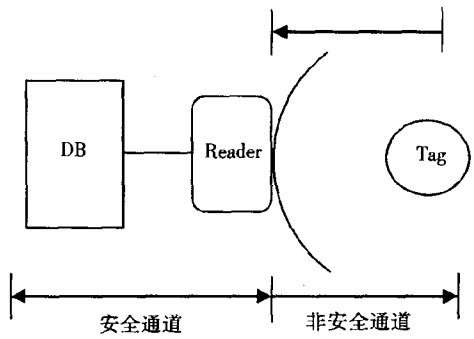

图1 RFID系统组成

Fig. 1 The composition of the RFID system

更广泛的发展,在设计RFID协议的时候应该满足如下安全特性:

(1)双向认证

读卡器向标签发出询问,标签对之作出响应,发送消息给读卡器,进而传递给服务器。服务器检索数据库中与标签相关的数值和与标签共享的秘密参数对标签进行认证,如果收到的消息,与计算的值相等,则标签被认证;认证够过后,服务器或读卡器会计算出一个密码值,并把相关参数一起发送给标签,标签利用本身存储的数据验证来自读卡器的消息,如果计算的值与发送的值相等,则读卡器被认证。

(2)流量分析

攻击者对读卡器和标签的信息截取,记录每次它们之间传递的数据,分析,提取有用信息。攻击者还可以冒充读卡器向标签发送多次的询问请求,并且截获标签返回的结果。从获得的数据中分析出自己想要的数据,达到伪造标签或者跟踪标签的目的。

(3)不可区分性

安全的RFID系统要求攻击者无法分辨标签每次的输出(无法对标签进行跟踪)。这就要求攻击者一方面即使获得了多个不同标签的输出,也无法区分出是某一张标签的输出;另一方面即使截获了来自于同一张标签的多次输出,同样无法区分是标签某次的输出。这一安全属性是RFID系统的基本安全需求。

(4)重传攻击

在读卡器发出认证请求时,攻击者偷听获取到标签的响应。在下一论的认证过程中,攻击者发送已获得的数据至读卡器,从而通过认证。因此,RFID系统必须具有应对重传攻击的能力。

(5)哄骗攻击

所谓的哄骗与复制攻击就是攻击者通过冒充读卡器,参与认证过程,截获有用信息,并且不被用户和服务器发现的过程;或者攻击者对标签侦听,记录下它的回应消息,并在稍后重放这个回应消息,从而达到冒充标签哄骗服务器的目的。

(6)同步

为了达到RFID系统的安全需求,很多RFID认证协议都对每次认证后的标签和数据库中的标签*ID*和密钥进行同步更新,进而适应分布式环境的需求。如果同步机制不严谨,同步更新就会遭到破坏,将造成合法标签也无法正常使用。

另外,其他研究这还提出RFID也要满足前向安全、匿名等安全需求。

2 相关协议的安全性分析

在先前提出的RFID安全方案中,比较典型的是Hash锁协议[1]、随机Hash锁协议[2]、Hash链协议[3]。随后,一些学者指出它们存在某些缺陷。Hash锁协议中标签的*ID*没有动态更新,致使meta*ID*始终保持不变,而且标签*ID*是以明文的形式传送。因此Hash锁协议很容易受到假冒攻击、重传攻击和追踪。为了解决Hash锁中位置跟踪的问题,Weis等人提出了随机Hash锁协议。虽然协议防止了对标签进行位置追踪,但是数据库对标签认证以后,带有明文*ID*的数据仍需通过不安全信道传送。因此,攻击者可以通过截获*ID*,通过流量分析对标签进行有效地追踪、假冒和对服务器进行重传攻击。在之后的Hash链协议协议中虽然解决了一些安全问题,但是协议只能对标签身份进行实体认证,而且也很容易受到重传和假冒攻击。

JeaCheol等人提出了一个基于Hash函数的RFID认证协议[8],本文称之为Hash-1协议。在协议中,协议的作者使用一个变量*SYNC*来解决数据库和标签中的*ID*更新的同步问题,在安全性方面能够抵抗大部分攻击。但是,通过分析,我们发现协议有个漏洞,最终导致它不能抵抗标签伪造攻击。协议中使用的参数如表1所示。

标签在通过第i次认证以后,标签和数据库服务器的参数值如表的第一行所示。在$i+1$次认证时,攻击者冒充读卡器向标签发起认证请求,并发送随机数($r_R=0$)给标签,标签检查$SYNC=0$,计算$P=H(ID_i)$,并发送P和随机数r_T给读

卡器。伪造的读卡器把 $P, r_R = 0, r_T = 0$ 传递给数据库服务器。标签能够正常通过服务器的认证。随后,服务器更新相关参数的值,具体如第 2 行所示。更新后的 ID 用 ID_j 表示。最后,服务器将 $Q = H(ID_i \| 0)$ 发送给读卡器,读卡器转发给标签。因为非法读卡器伪造和篡改了两个随机数的值($r_R = 0, r_T = 0$)。因此,服务器没有办法通过标签的认证。但是攻击者可以截获 Q 的值,而它恰恰是服务器通过标签认证后,标签中 ID 的值。因此,攻击者就可以伪造标签,并且可以通过服务器的认证。

表 1　Hash - 1 协议的参数表

Table 1　The parameters of the protocol

DB Server 参数			Tag 参数	
ID	*HID*	*PID*	*ID*	*SYNC*
ID_i	$H(ID_i)$	$ID_i ID_i$	0	
$ID_j = H(ID_i \| 0)$	$H(ID_j)$	$ID_i ID_j$		

Seo - Baek 等人提出了一个基于 EPCGen2 标准的 RFID 认证协议[9]。经过分析研究,我们发现它同样有安全缺陷,容易受到重传攻击。问题的主要原因是随机数是标签一方提供的,而且协议本身没有同步控制机制。首先,读卡器向标签发起查询(Query)。标签计算 $V_T = \mathrm{CRC}(\mathrm{EPC} \| N_1) \oplus N_2$,发送 V_T, N_1, N_2 给读卡器,读卡器将它们转发给服务器,服务器通过消息验证码 CRC 验证的 V_T 完整性,进而认证标签。然后,服务器计算 $\alpha_R = \mathrm{CRC}(\mathrm{EPC} \| N_1)$, $\beta_R = \mathrm{CRC}(\mathrm{EPC} \| N_2)$, $V_R = \alpha_R \oplus \beta_R$。发送 V_R 给读卡器,读卡器将之传递给标签。标签通过计算,可以认证读卡器的合法性。攻击者只要每次记录标签发送的参数,就可以冒充标签通过服务器的认证,因为随即参数是由标签一方提供的,而且对随机数没有任何保护措施。

本文把我们对上述两个协议的分析结果和一些典型的协议在安全性方面进行了比较,详见表 2。

表 2　协议安全性比较

Table 2　The security comparison of the protocol

协议	双向认证	流量分析	哄骗攻击	重传攻击	不可区分性	同步
Hash 锁	×	×	×	×	×	×
随机 Hash 锁	×	×	×	×	×	×
Hash 链	×	√	×	×	√	×
Hash - 1	√	×	×	√	√	√
EPCGen2 - 1	√	√	√	×	√	×

3　结 论

目前对 RFID 安全技术研究还处于刚起步阶段,要真正达到实用的效果和解决 RFID 在实际应用中面临的安全问题还需要进行大量深入研究。之前研究者们提出的认证协议大部分都能达到双向认证的目的,但是经过分析,它们在某些方面都有一些缺陷。为了使 RFID 技术更加成熟和实用,提出了 EPCGen2 标准。此标准符合低成本的标签的要求(通常来讲,低成本 RFID 标签包含 5 000 ~ 10 000 个门电路[10],可用于安全机制的是 400 ~ 4 000 个门电路[11]),而对低成本标签的安全性提高也是一个挑战。目前符合标准的认证协议也都存在一些安全问题。

如何设计一个安全的 RFID 认证协议,并且还要符合低成本标签的要求成了一个广泛研究的课题,本文对新提出的两个 RFID 认证协议进行了安全性分析,发现它们在某些方面都存在安全缺陷。随着电子芯片集成化的进一步提高和学者们的广泛研究,相信低成本和高安全的矛盾会很快得到解决。

参考文献:

[1] Sarma S E, Weis S A, Engels D W. RFID systems and security and privacy implications[J]. Lectures Notes in Computer Science 2523. Berlin: Springer - Verlag, 2003:454 - 469.

[2] 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.

[3] Weis S A, Sarma S E, Rivest RL. Security and privacy aspects of low - cost radio frequency identification systems[C]. Lectures Notes in Computer Science 2802. Berlin: Springer - Verlag, 2004:201 - 212.

[4] EPC Class 1 Gen 2 st an dard[EB/OL]. http: //www. epcglobalinc. org/standards/ uh f c1g2/.

[5] Duc D N, Park J, Lee Hyunrok, et al. Enhancing Security of EPCglobal GEN - 2 RFID Tag Against Traceability and Cloning[C]//Proc. of the 2006 Symposium on Cryptography and Information Security. Beijing, China,2006.

[6] Chien Hungyu, Chen Chehao. Mutual Authentication Protocol for RFID Conforming to EPC Class 1 Generation 2 Standards [J]. Computer Standards &Interfaces, 2007,29(2):254 - 259.

[7] Konidala D M, Kim K. RFID Tag - Reader Mutual Authentication Scheme Utilizing Tag's Access Password[Z]. Auto - ID Labs White Paper,2007.

[8] JeaCheol Ha, SangJae Moon, Juan Manuel Gonzalez Nieto, Colin Boyd. Low - Cost and Strong - Security RFID Authentication Protocol[J]. Lecture Notes in Computer Science, LNCS 4809, 2007:795 - 807.

[9] Seo D, Baek J, Cho D. Secure RFID Authentication Scheme for EPC Class Gen2[C]. In Proc. 3rd Int. Conf. on Ubiquitous Information Management and Communication ICUIMC - 2009:221 - 227.

[10] Peris - Lopez P, César Hernández Castro J, Estévez - Tapiador J M, et al. RFID systems: A survey on security threats and proposed solutions[C]//Proc of the IFIP - TC6 11th Int Conf on Personal Wireless Communications. Berlin: Springer, 2006:159 - 170.

[11] Ranasinghe D, Engels D, Cole P. Low - cost RFID systems: Confronting security and privacy[C]//Proc of the Auto - ID Labs Research Workshop. Cambridge, MA: Auto - ID Labs, 2004.

Security Analysis of RFID Authentication Protocol

WANG Ming-hui[1,2], ZHENG Zhou[2], TANG Yong-zheng[1,2]

(1. School Information Technolog, Yancheng Institute of Technology, Yancheng Jiangsu 224051, China;
2. Modern Educational Technology Center, Yancheng Institute of Technology, Jiangsu Yancheng 224051, China;)

Abstract: For security issues of RFID authentication protocol, this paper analyzes the advantages and disadvantages of recently proposed several protocols and gives some comparisons of the security properties. The results show that there are some security flaws in some respects. Through research and analysis on the protocol, some authentication protocols currently proposed do not meet certain security requirements of RFID systems. Only through an effective way to design a protocol, it will meet more reliable, secure and efficient protocal.

Keywords: Radio Frequency Identification (RFID); authentication; privacy; security protocol

(责任编辑:沈建新)