第33卷 第21期 计 算 机 工 程 2007年11月
Vol.33 No.21 Computer Engineering November 2007
·安全技术· 文章编号：1000—3428(2007)21—0128—02 文献标识码：A 中图分类号：TP393

RFID应用系统中的Tag-reader安全通信协议

高 磊，盛焕烨
(上海交通大学电子信息与电气工程学院，上海 200030)

摘 要：无线射频识别(RFID)技术目前已被广泛应用，但其缺乏安全机制，无法有效地保护RFID标签中的数据信息。该文分析了RFID技术在应用中存在的安全及隐私问题，提出了在RFID标签芯片计算资源有限的情况下解决这些问题的一个安全通信协议。该协议利用Hash函数技术实现了防止消息泄漏、伪装、定位跟踪等安全攻击。

关键词：无线射频识别；安全；通信；Hash；攻击

Tag-reader Secure Communication Protocol in RFID Application System

GAO Lei, SHENG Huan-ye
(School of Electronic, Information and Electrical Engineering, Shanghai Jiaotong University, Shanghai 200030)

【Abstract】 Radio frequency identification(RFID) technology has been wildly used, but it is lack of security mechanism and it can not protect its data effectively. By analyzing the security and privacy problems in RFID application, this paper affords a secure communication protocol under the limited computation resources in RFID tag to solve these problems. The protocol adopts Hash function to avoid security attacks such as information leak, counterfeit, orientation tail, etc.

【Key words】 radio frequency identification (RFID); security; communication; Hash; attack

1 无线射频识别技术简介

无线射频识别技术(radio frequency identification, RFID)或称电子标签技术是从二十世纪六七十年代兴起的一项非接触式自动识别技术。它利用射频方式进行非接触双向通信，以达到自动识别目标对象并获取相关数据的目的，具有精度高、适应环境能力强、抗干扰性强、操作快捷等许多优点。最基本的RFID系统主要由下面3部分组成：

(1)标签(tag)：又称电子标签、智能卡、识别卡或标识卡，由嵌入式微处理器及其软件、卡内发射与接收天线、收发电路组成。标签为信息载体，含有内置天线，用于和射频天线间进行通信。

(2)阅读器(reader)：读取/写入标签信息的设备。

(3)后台数据库(backend)：用于存储标签标识所对应的相关数据。

一般情况下，阅读器和后台数据库之间的通信可以认为是安全可靠的，本文将二者等同看待。

2 RFID面临的安全问题

无线射频识别技术的应用虽然十分广泛，但其存在一个不可忽视的隐患——安全机制。没有可靠的安全机制，就无法有效保护RFID标签中的数据信息。目前，RFID的安全性已经成为制约RFID广泛应用的重要因素。针对RFID的主要安全攻击可简单地分为主动攻击和被动攻击2种类型[1]。

主动攻击主要包括：(1)从获得的RFID标签实体，通过逆向工程手段，进行目标RFID标签重构的复杂攻击；(2)通过软件，利用微处理器的通用通信接口，通过扫描RFID标签和响应阅读器的探询，寻求安全协议、加密算法以及它们实现的弱点，进而删除RFID标签内容或篡改可重写RFID标签内容的攻击；(3)通过干扰广播、阻塞信道或其他手段，产生异常的应用环境，使合法处理器产生故障，拒绝服务的攻击等。

被动攻击主要包括：通过采用窃听或非法扫描等技术，获得RFID标签和识读器之间或其他RFID通信设备之间的通信数据，跟踪货品流通动态等。

攻击者通过对RFID系统中的标签、标签中存储的数据以及标签与阅读器之间的通信实施主动攻击或被动攻击，将使RFID系统面临非常巨大的安全风险。

RFID系统中最主要的安全风险是“数据保密性”。显然，没有安全机制的RFID标签会向邻近的识读器泄漏标签内容和一些敏感信息。由于缺乏支持点对点加密和PKI密钥交换的功能，在RFID系统应用过程中，攻击者有许多机会可以获取RFID标签上的数据。RFID系统中的另一个安全风险是“位置保密性”。如同个人携带物品的商标可能泄漏个人身份一样，个人携带物品的RFID标签也可能会泄漏个人身份，通过识读器就能跟踪携带系列不安全RFID标签的个人。

此外，攻击者还可以利用伪造标签代替实际物品来欺骗货主，使其误认为物品还在货架上。攻击者也可能通过篡改RFID标签上的数据，用低价物品标签替换高价物品标签，以此来获取非法利益。

3 基于Hash函数的安全通信协议

为了解决RFID系统的安全问题，最大限度地降低其面临

作者简介：高 磊(1978－)，男，硕士研究生，主研方向：RFID技术及其应用；盛焕烨，教授、博士生导师

收稿日期：2006-11-25 **E-mail：**gaolei@sjtu.edu.cn

的安全风险，必须为RFID系统构造一个可靠的安全机制，用于tag与reader间的相互认证和传输数据。所有的安全机制都需要建立在一个加密算法的基础之上[2]。但由于RFID标签的使用数量大、范围广，必须将其造价控制在比较低廉的水平，这使得RFID标签通常只能拥有大约 5 000 个~10 000 个逻辑门，而且这些逻辑门主要用于实现一些最基本的标签功能，仅剩少许可用于实现安全功能。但实现AES(advanced encryption standard)算法需要大约 20 000 个~30 000 个逻辑门[3]，实现RSA、椭圆曲线密码等公钥密码算法则需要更多的逻辑门。因此，大多数RFID标签根本无法提供足够的资源来实现一些比较成熟和先进的加密算法，而只能采用一些“PIN码”或“password”机制来保护秘密数据。

按照目前已有的技术和芯片制造水平，在 tag 标签芯片中实现 SHA-1 等成熟 Hash 算法大约需要 3 000 个~4 000 个逻辑门，因此，本文提出了基于 Hash 函数的安全通信协议，用于保证 tag 和 reader 之间数据传输的安全性，同时防止在传输时泄漏 tag 所携带的个人信息和位置信息。

3.1 协议中的 Hash 函数

在本协议中需要用到 2 个Hash函数：H和G，这 2 个Hash函数的实现是可以公开的，无须保密。而且，H和G理论上可以是同一算法，但是考虑到H仅用于计算一个标签标识串的Hash值，可以采用比较简单的算法，而G要用于计算tag和backend间互相鉴别和传输会话密钥时的Hash值，因此，应该采用安全强度较大的Hash算法。显然，作为Hash函数，H和G均应满足[4]：

(1)对于任意长度的消息 M，H 和 G 返回固定长度 m 的函数值 $h=H(M)$或 $G(M)$；

(2)给定 M 很容易计算出 h，甚至在 RFID 芯片上计算资源有限的条件下也是如此；

(3)给定 h，很难还原出 M，即使知道 H 和 G 的算法也是如此；

(4)对于特定的 M，很难找到另一个 M'，使得 $H(M)=H(M')$，即使知道 H 和 G 的算法也是如此。

3.2 协议的初始化

协议要求在使用前对 backend 的数据库和系统所使用的 tag 进行初始化操作。

(1)tag端：tag中被写入初始值由 3 部分构成：1)私密信息 S_0，如EPC条码等可供识别tag的标识；2)计数器初值C_0；3)会话密钥R_0。

(2)backend端：其数据库中保存有一张所有tag的表单，表单记录有每个tag所对应的S_0、会话密钥R_0、S_0的当前值S^i(等于S_0)和backend端计数器值 C_b^i (等于C_0)。

3.3 协议的算法步骤

(1)backend 向 tag 发送 R/W 请求。

(2)tag 向 backend 返回标签当前计数器的值 C_t^i 和 $G_t\{S_t^i \oplus C_t^i\}$。

(3)backend获得 C_t^i 后，对数据库tag表单中每个 $C_b^i \le C_t^i$ 的tag所对应的S^i执行$S^{i+1}=H\{S^i \oplus R_{i-1}\}$运算 $C_t^i - C_b^i$ 次，以得到 S_b^i，然后计算$G_b\{S_b^i \oplus C_t^i\}$，backend将每一个tag所对应的$G_b$与$G_t$相比较，当且仅当 $S_t^i = S_b^i$ 时，$G_b=G_t$。由此可知，如果存在某一$G_b=G_t$，则证明该标签属于backend端数据库所保存的tag表，backend完成对tag的鉴别，同时更新数据库中该tag对应的 C_b^i 为 C_t^i+1。

(4)一旦backend完成对tag的鉴别，就产生一个随机数R_i作为会话密钥，并将数据库中该tag对应的会话密钥更新为R_i，S^i更新为$H\{S_b^i \oplus R_i\}$，同时还要计算出$R_i \oplus G\{S_b^i\}$, $G\{R_i \oplus S_b^i\}$，并将这二者发送给tag。

(5)tag计算$G\{S_t^i\} \oplus R_i \oplus G\{S_b^i\}$以得到$R_t$，并由此进一步计算得出$G^*\{R_t \oplus S_t^i\}$，当且仅当$R_t=R_i$以及 $S_t^i = S_b^i$ 时，$G^*\{R_t \oplus S_t^i\}= G\{R \oplus S_b^i\}$。由此tag完成对backend的鉴别，同时得到会话密钥R_i用于tag与Reader间其他数据的传输，同时更新tag中保存的会话密钥R_{i-1}为R_i。

(6)无论(3)~(5)是否成功执行，tag均更新 $S_t^{i+1} = H\{S_t^i \oplus R_t\}$，$C_t^{i+1} = C_t^i + 1$。

4 协议安全性分析

根据本文所提供的安全通信协议，可以对 RFID 系统面临的一些安全风险进行分析评估。

(1)对 tag 的攻击。攻击者试图伪装成一个合法的 reader，但由于攻击者不知道 S_b^i，因此其无法构造出与 G^*相等的 G，这种伪装将被 tag 识破。

(2)对backend的攻击。攻击者试图伪装成一个合法的tag，但由于攻击者不知道 S_t^i，因此其无法构造出与G_b相等的G_t，这种伪装将被backend识破。

(3)replay攻击。攻击者记录下第i次tag与backend间的通信信号，企图利用重放tag在(2)中向backend传输的数据伪装成一个合法的tag。由于在i+1 次tag与backend间通信时，tag应该向backend发送 C_t^{i+1} 和$G_t\{S_t^{i+1} \oplus C_t^{i+1}\}$，攻击者的重放将是无效数据。

(4)对tag私密性的保护。因为协议约定无论(3)~(5)是否成功执行，tag均更新 $S_t^{i+1}=H\{S_t^i \oplus \mathrm{R_t}\}$，$C_t^{i+1}=C_t^i+1$，所以无论reader是否合法，其每次读到的tag数据 C_t^i 和$G_t\{S_t^i \oplus C_t^i\}$都是不同的，而且由于得不到$R_t$，攻击者无法将本次读到的 C_t^i 和$G_t\{S_t^i \oplus C_t^i\}$和以前读到的 C_t^i 和$G_t\{S_t^i \oplus C_t^i\}$关联起来。也就是说，如果没有backend端的数据库中保存的tag表，攻击者根本无从判断 2 次读到的数据是否属于同一个tag。

(5)对通信内容的保护。因为协议首先对 tag 和 backend 进行了相互认证，通过认证的双方在协议的第(4)步进行了会话密钥的传递，而且此密钥将用于本次会话时的数据传输加密，所以攻击者即使能够窃听到 tag 和 reader 之间的通信数据，也无法获取其真实内容。

5 结束语

目前已有不少关于 RFID 系统的安全问题的协议和方案公开发表，但是其中的绝大多数只是针对安全问题的某些方面，并没有一个成熟的完整解决方案。而另一方面，受到被动式标签芯片性能和运算能力的限制，一些比较成熟和先进的加密算法如 AES、RSA、椭圆曲线密码等近期内还无法运用到 RFID 标签的加密中。

本文提出的 RFID 安全通信协议基于传统的 challenge-response 框架，其采用的 Hash 函数对标签芯片的计算能力要求较低，比较适用于目前的实际情况和成本控制目标。同时，该协议的框架具有向后兼容公钥密码体制的特性，当今后标签芯片性能可以支持某些公钥密码算法时，可以方便地将 Hash 函数部分改为公钥密码算法，而对于协议的执行步骤，只须做少许改动即可。

（下转第 133 页）