文章编号:1001 - 9081(2011)03 - 0805 - 03
doi:10.3724/SP.J.1087.2011.00805

结合 Hash 函数和密钥阵列的 RFID 安全认证协议

谢 川
(重庆工商大学 计算机科学与信息工程学院,重庆 400067)
(chuanxie@yeah.net)

摘 要:无线传输、信号广播、资源受限等特点使无线射频识别(RFID)技术存在潜在的安全隐患。在分析目前常见的 RFID 认证协议基础上,提出一种结合单向 Hash 函数和密钥阵列的安全认证协议。新协议在认证过程中使用单向 Hash 函数值代替标签标识符 ID,并为每一对阅读器和标签之间设计独立的认证密钥,在抵抗包括窃听、位置跟踪、重传攻击、拒绝服务和篡改等多种攻击的基础上,进一步增强了标签信息的私密性,对抵御来自系统内部的威胁具有明显的优势。

关键词:无线射频识别;标签;阅读器;后台服务器;认证协议;哈希函数
中图分类号:TP309.7 **文献标志码**:A

RFID authentication protocol based on Hash function and key array

XIE Chuan
(*College of Computer Science and Information Engineering, Chongqing Technology and Business University, Chongqing* 400067, *China*)

Abstract: Wireless transmission, broadcast of signals, resource-constraint disturb the reliability of Radio Frequency Identification (RFID) system and block the deployment progress of RFID techniques. Through the analysis of current common RFID authentication protocol, an authentication protocol based on Hash function and key array was proposed. The new protocol used one-way Hash function value instead of label identifier, and designed independent authentication key for each pair between the reader and the tag in the certification process. It could resist several possible attacks, including eavesdropping, location tracking, re-transmission attacks, Denial of Service (DoS), tampering and other attacks. It has obvious advantages in enhancing the tag identity privacy, and resisting the threat from within the system.

Key words: Radio Frequency Identification (RFID); tag; reader; back-end server; authentication protocol; Hash function

0 引言

典型的无线射频识别(Radio Frequency Identification, RFID)系统由 RFID 标签(简称标签)、RFID 阅读器(简称阅读器)和后台数据库(后台服务器)组成,如图 1 所示。标签有自己的存储器和计算单元,使其可以具有访问控制和加密功能,这样就可以让标签应用于许多重要领域,如供应链管理、金融系统、矿井安全管理等。随着 RFID 能力的提高和标签应用的日益普及,安全问题特别是用户隐私问题变得日益突出,用户如果带有不安全的标签产品,则在用户没有感知的情况下,被附近的阅读器读取,从而泄露个人的敏感信息。因此,在 RFID 应用时,必须仔细分析所存在的安全威胁,研究和采取适当的安全措施。由于标签的低成本、低功耗应用需求,它无法实现复杂的高安全性的加密算法,使得大量研究人员都投身于 RFID 安全认证协议的研究中,目前具有代表性的有 Hash-Lock[1]、Hash 链[2]、分布式询问-应答协议[3]、NTRU 公钥加密[4]等。但所有的这些认证协议都忽略了来自系统内部的合法阅读器和合法标签之间的伪造与篡改问题。本文针对这一安全隐患,提出一种结合 Hash 函数和密钥阵列的安全认证协议。

1 有关 RFID 认证协议分析

对于目前已提出的 RFID 安全认证协议,主要从以下几个方面进行设计和实现。

1.1 基于 Hash 函数的 RFID 认证协议

基于 Hash 函数的 RFID 认证协议有很多种,其基本思路是用标签标识符 ID 的 Hash 函数值作为虚拟 ID 来应答阅读器的查询,并且在每次通信时,服务器都更新标签的虚拟 ID,用标签虚拟 ID 的变化来保证 RFID 的私密性,真实的标签 ID 存储在后台数据库。该协议可以有效防止窃听、重放攻击和位置追踪攻击,其缺点是无法避免阻断攻击,如果标签和阅读器的通信被恶意阻断,导致标签的虚拟 ID 不能更新,或者服务器与标签不能同步更新,进而威胁整个系统的工作。

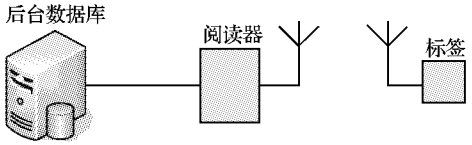

图 1 RFID 系统基本构成

1.2 基于状态的 RFID 认证协议

基于状态的 RFID 认证协议可以保证 RFID 系统通信被非法结束时仍具有安全性。该协议中的标签有一个标记 tag(值只能为 0 或者 1),它表明上一次通信是否安全结束(tag = 0,表示安全结束,否则为异常结束)。根据标记 tag 的值,标签可以判断上一次通信是否正常结束,从而防止标签 ID 非同步更新攻击。该协议仍然利用单向 Hash 函数的安全性来防止窃听攻击,用每次通信产生新的随机数和标签 ID 的

收稿日期:2010 - 08 - 18。 **基金项目**:重庆市科技攻关项目(CSTC2010AA2036)。
作者简介:谢川(1971 -),男(土家族),重庆黔江人,讲师,硕士研究生,主要研究方向:网络与通信、物联网。

更新来防止重放攻击和位置追踪攻击。然而,如果最后一次通信被恶意阻断,仍然会出现后台数据库的标签 ID 和 RFID 标签的 ID 非同步问题。

1.3 基于密钥加密的 RFID 认证协议

为了给 RFID 系统提供更好的安全性和私密性,人们开始把密钥系统引入 RFID 认证协议中。一种基于对称密钥体系的请求-应答认证协议是所有标签与阅读器之间共享同一个密钥,一旦某个标签的密钥被泄露,就会破坏整个系统。近年来又有研究表明基于公钥加密系统的 RFID 认证协议可以提供更好的安全性和私密性[5],并且研究出具体的协议实现方式[4,6],标签使用公钥进行加密,服务器使用私钥进行解密,但它仍然不能解决来自系统内部的攻击。另外,标签只有有限的存储空间和计算能力,并具有较高的能量和成本限制,而一般的公钥加密算法对存储空间和计算能力都有较高的要求,即使是 NTRU(Number Theory Research Unit)加密算法也对 RFID 标签提出了较高的要求。

2 提出的协议

值得注意的是,以上协议都忽略了一个安全隐患,即来自 RFID 系统内部的合法标签和阅读器之间的伪造和篡改问题。解决这个问题的方法就是在共享密钥的基础上,给每一对阅读器和标签之间分配一个认证密钥,即任意一个阅读器和任意一个标签之间的通信都有唯一的认证密钥。系统还使用单向 Hash 函数的不可逆特性,防止密钥被截取所带来的隐患。

2.1 密钥阵列

阅读器与后台数据库之间是通过安全信道连接的,安全威胁主要来自于标签和阅读器之间的无线信道。为了保证不同阅读器和标签之间具有唯一的认证密钥,除了所有阅读器和标签之间拥有共享密钥 K_u 之外,还构造一个 $N \times M$ 的密钥矩阵 $\boldsymbol{K}$,其中 N 为系统中阅读器的数量,M 为系统中标签的数量,矩阵 $\boldsymbol{K}$ 如式(1)所示。

$$\boldsymbol{K} = \begin{bmatrix} K_{11} & K_{12} & \cdots & K_{1M} \\ K_{21} & K_{22} & \cdots & K_{2M} \\ \vdots & \vdots & & \vdots \\ K_{N1} & K_{N2} & \cdots & K_{NM} \end{bmatrix} \tag{1}$$

矩阵元素 K_{ij} 表示第 i 个阅读器和第 j 个标签之间的认证密钥,该矩阵存放在系统后台数据库中,即使系统庞大使得该矩阵中的元素太多也不用担心存储能力和密钥查找速度。标签初始化时,在标签的存储器中保存所有阅读器的 ID 和该阅读器与自己对应的认证密钥表,如表 1 所示。因为阅读器的数量远不及标签数量多,使得表 1 对存储能力和查找速度要求不是太高,RFID 能够实现。

表 1 RFID 标签 j 中存放的密钥

序号	阅读器 ID	密钥
1	ID_1	K_{1j}
2	ID_2	K_{2j}
⋮	⋮	⋮
N	ID_N	K_{Nj}

2.2 单向 Hash 函数

为了避免在认证过程中传递的标签的 ID 标识符被攻击者识别,服务器使用一个单向 Hash 函数 $h(x)$,对每个标签的 id_j 标识符计算 $u_j = h(id_j)$,id_j 表示第 j 个标签的 ID 标识符,u_j 表示第 j 个标签的 $h(x)$ 函数值。标签认证时使用 u_j 代替其 ID 标识符,即使被攻击者获取也不知道是哪一个标签在进行认证通信。系统初始化时将 u_j 存储到对应标签的存储器中,同时将所有标签的 $h(x)$ 函数计算结果保存在服务器的存储器中,如表 2。

表 2 后台数据库存放的标签 ID 的 Hash 函数值

序号	标签 ID	$h(x)$ 的值
1	id_1	u_1
2	id_2	u_2
⋮	⋮	⋮
M	id_M	u_M

2.3 协议认证过程

为不失一般性,这里仍使用第 i 个阅读器和第 j 个标签来描述协议的认证过程。

1)阅读器 i 首先产生一个随机数 R_i,并与自己的标识符 ID_i 一起,通过共享密钥 K_u,加密成认证请求 $E_{K_u}(R_i \| ID_i)$,把认证请求发送给标签 j。

2)标签 j 收到认证请求后,使用共享密钥 K_u 解密,获得到 R_i 和 ID_i,在自己的存储单元中查找对应的 ID_i,若找不到该 ID_i,则终止响应。如果能够查找到对应的 ID_i,则从表 1 中查找与之对应的 K_{ij}。同时,标签产生随机数 R_j,并与接收到的随机数 R_i 一起,加密成数据块 $E_{K_{ij}}(R_i \| R_j)$,并与自己存储的 id_j 的单向 Hash 函数值 u_j 一起,用共享密钥 K_u 加密成 $E_{K_u}(u_j \| E_{K_{ij}}(R_i \| R_j))$ 作为认证响应发送给阅读器 i。

3)阅读器收到标签的响应后,使用共享密钥 K_u 进行解密,并将解密得到的 u_j 和自己的 ID_i 组合到一起发送给后台数据库服务器。因为阅读器与服务器之间是安全信道,这里的数据传送不需加密。

4)服务器收到阅读器传来的数据后,提取出 u_j,并在表 2 中进行查找,如果没有找到 u_j,则告诉阅读器认证失败。如果找到合法的 u_j,则从表 2 中查找到对应的 id_j,并从密钥阵列中查找出对应的密钥 K_{ij},并将 K_{ij} 传给阅读器 i。

5)阅读器 i 得到 K_{ij} 后,即可解密 $E_{K_{ij}}(R_i \| R_j)$ 得到 R_i 和 R_j。如果 R_i 与认证发起时阅读器产生的 R_i 相同,则完成阅读器对标签的认证,否则认证失败。

6)阅读器计算 $R_i \oplus R_j$,并用 K_{ij} 进行加密得 $E_{K_{ij}}(R_i \oplus R_j)$,把加密后的数据发送给标签,标签使用 k_{ij} 解密后,对比解密出的 $R_i \oplus R_j$ 与认证请求时阅读器 i 发过来的 R_i 和自己产生的随机数 R_j 的异或结果是否相同,如果相同,则完成标签 j 对阅读器 i 的认证,否则认证失败。阅读器 i 不直接使用 $E_{K_{ij}}(R_i \| R_j)$ 发送给标签 j,可以避免攻击者截获第 2)步标签 j 的响应,而在不知道 R_i、R_j 和 K_{ij} 的情况把截获到的部分数据直接返送给标签 j,造成标签 j 对阅读器 i 的错误认证。

通过上述认证过程,可以看出整个系统有共享密钥 K_u 保护,而具体实现认证还依赖认证密钥 $K_{i,j}$ 和单向 Hash 函数值保护,即 3 重防护来保障认证安全。

3 安全性分析

本文提出安全认证协议可以有效地保护标签信息的隐私,提供阅读器和标签间的双向认证,并能防止非法攻击,如窃听、位置跟踪、重传攻击、流量分析攻击等。

1)标签信息的隐私保护。对于来自非本系统的攻击者而言,不知道本系统的认证过程,也不知道本系统的共享密钥 K_u,也就不能跟标签建立起联系进而攻击,即使盗取了共享密钥和认证过程,也不能知道各个阅读器和标签之间对应的认

证密钥 K_{ij}。另外，标签中保存的标识符 $u_j = h(id_j)$，由于 $h(x)$ 是单向 Hash 函数，万一 u_j 在传输过程中被识别，非法用户不可能由此知道真实的标签标识符 id_j，只有合法的后台服务器通过查找数据库才能得到标签的真实标识符 id_j。

2）双向认证。由前文的协议认证过程可知，阅读器与标签的认证是相互的，在实现阅读器对标签的认证成功后，还要实现标签对阅读器的认证，只有双向都认证成功才被当做一次认证成功。双向认证增强了认证的可靠性。

3）窃听和流量分析。由于阅读器和标签之间的通信是不安全信道，非法用户可以访问该信道。在该协议中，标签向阅读器发送的是用 K_u 和 K_{ij} 加密的信息 $E_{K_u}(u_j \| E_{K_{ij}}(R_i \| R_j))$，阅读器向标签有时是 K_u 加密的信息 $E_{K_u}(R_i \| ID_i)$，有时是 K_{ij} 加密的信息 $E_{K_{ij}}(R_i \oplus R_j)$，获取明文不仅仅需要解密的密钥，而且还需知道通信信息是哪种类型的数据，因此非法用户不能窃听到明文。另外，每次传递的信息数据都包含随机数 R_i 和 R_j 的不同组合，加密结果随着随机数的内容和长度而变化，非法用户不能进行流量分析攻击。

4）重传攻击。在 RFID 中，重传攻击主要包括两种方式：一种是伪装成阅读器，重传阅读器对标签的认证请求；另一种是伪装成标签，重传标签对阅读器的认证响应。本协议在阅读器传给标签的信息和标签传给阅读器的信息中都包含随机数 R_i 和 R_j 的组合，通过对比发送和接收的随机数 R_i 和 R_j 是否一致，就可识别出攻击者的重传行为。

5）标签位置跟踪攻击。攻击者经常伪装成阅读器发来认证请求，诱骗标签发送认证响应，再根据响应的内容来确定是否是同一标签的响应，当判断出是同一标签在不同时刻的响应时，就可确定同一标签在不同时刻所处的位置，进而实现对标签的定位跟踪。在本协议中，合法的阅读器发送的认证请求信息为 $E_{K_u}(R_i \| ID_i)$，因此，攻击者必须首先具有合法的阅读器 ID 标识符信息，如果是非法的阅读器ID号，标签在存储器中找不到该ID数据时，不会响应此次认证请求。其次，攻击者必须知道共享密钥 K_u，否则，标签使用共享 K_u 不能解密出 $R_i \| ID_i$。即使攻击者的认证请求信息合法，标签对不同时刻的认证请求也有不同的响应，如第一时刻的响应为 $E_{K_u}(u_j \| E_{K_{ij}}(R_i \| R_j))$，第二时刻的响应为 $E_{K_u}(u_j \| E_{K_{ij}}(R_i \| R_j'))$，因两次响应的随机数不同（$R_j \neq R_j'$），也使得 $E_{K_u}(u_j \| E_{K_{ij}}(R_i \| R_j)) \neq E_{K_u}(u_j \| E_{K_{ij}}(R_i \| R_j'))$，攻击者不能断定是同一个标签的响应信息，不能进行位置跟踪攻击。

6）拒绝服务攻击。拒绝服务也称做阻断攻击，即合法的标签不响应阅读器的认证请求，合法的阅读器不回复标签的响应。攻击者向无线通信信道发送干扰信号，使得合法的标签无法正确接收阅读器的认证请求，合法的阅读器无法正常接收标签的响应信息，从而导致认证失败，本协议不能避免攻击者发送干扰信号干扰数据，但可以实现不发生错误认证。

7）篡改攻击。篡改攻击是指攻击者收到空间信息后，修改信息内容再发送出去的攻击方法，这种攻击方式相当于让接收方收到两次来自于同一信源的信息，因本协议能避免重传攻击，可有效防止这种篡改行为。即使接收方没有收到合法信息，只收到篡改后的信息，也不会受到影响，因为攻击者不知道认证密钥和加密方式，无法将信息篡改成另外一个合法的数据。例如攻击者想篡改标签的响应信息 $E_{K_u}(u_j \| E_{K_{ij}}(R_i \| R_j))$，因为不知道 K_u 和 K_{ij}，篡改后的信息不能被阅读器和后台服务器正确解密，导致认证不成功。

8）系统内部的合法阅读器攻击。对于系统内部的合法阅读器，其攻击方式除上述方式外，还有一种最隐蔽的攻击方式，即冒名攻击。因攻击者是系统内的合法阅读器，对通信协议、共享密钥、数据格式都非常清楚，可假冒其他合法阅读器来对标签进行攻击。假设系统内的合法阅读器 x 假冒阅读器 y 向标签 j 发送认证请求，发送时冒用阅读器 y 的标识 ID_y，发送的认证请求信息为 $E_{K_u}(R_x \| ID_y)$，标签 j 在收到该认证请求后识别出 ID_y，并从存储单元中查找到阅读器 y 跟自己之间的认证密钥 K_{yj}，加密成认证响应信息 $E_{K_u}(u_j \| E_{K_{yj}}(R_x \| R_j))$，阅读器 x 收到该响应信息后，可成功解密出 u_j，但不能推断出对应的标签标识 id_j。而且阅读器与后台服务器之间是安全信道，后台服务器不可能给阅读器 x 发送阅读器 y 与标签 j 之间的认证密钥 K_{yj}，因此阅读器 x 无法获得标签 j 的响应中的随机数 R_j。既不知道 K_{yj}，也不知道 R_j，也就无法计算出 $E_{K_{yj}}(R_i \oplus R_j)$ 来完成 2.3 节认证过程的第 6）步，即不能实现标签 j 对阅读器 x 的成功认证，即冒名不成功。

9）系统内部的合法标签攻击。同样道理，对于系统内的合法标签的攻击方式通常也是假冒其他标签。假设系统内部合法标签 p 假冒标签 q 响应阅读器 i 的认证请求，收到认证请求信息 $E_{K_u}(R_i \| ID_i)$ 后，因不知道标签 q 与阅读器 i 之间的认证密钥 K_{iq}，也不知道标签 q 的单向 Hash 函数值 u_q，因此无法计算出 $E_{K_u}(u_q \| E_{Kiq}(R_i \| R_q))$。如果使用标签 p 自己的 Hash 函数值和认证密钥，则计算出的信息为 $E_{K_u}(u_p \| E_{K_{ip}}(R_i \| R_p))$ 只能代表自己的情况，没有实现假冒攻击。如果直接使用标签 q 的标识符 id_q 和自己的认证密钥，则计算出的响应信息为 $E_{K_u}(id_q \| E_{K_{ip}}(R_i \| R_p))$，阅读器 i 收到此认证响应后，用共享密钥 K_u 解密可得到 id_q 和 $E_{K_{ip}}(R_i \| R_p)$，送后台服务器可发现 id_q 不是标签的 Hash 函数值，直接判定认证失败，不仅是冒名认证不成功，还可以找到攻击者。

综合前面的分析可知，本协议拥有很强的安全性，还可以抵制来自系统内部的攻击，表 3 给出了几种已公开发表的 RFID 安全协议[6-9]的对比。“T”代表协议具有本项功能，“F”代表协议不具有本项功能。

表 3　常用的几种 RFID 认证协议对比

认证协议	标签隐私保护	相互认证	窃听和流量分析	重传攻击	标签位置跟踪	拒绝服务	篡改	系统内部阅读器攻击	系统内部标签攻击
Hash-Lock	T	F	F	F	F	F	F	F	F
Hash 链	T	F	F	T	T	F	F	F	F
三通相互鉴别	F	T	F	T	T	T	T	F	F
分布式询问-应答	F	T	F	T	T	T	T	F	F
基于公钥加密	T	T	T	T	T	T	T	F	T
本协议	T	T	T	T	T	T	T	T	T

（下转第 811 页）

1)创建一个 SignedXml 对象,获取 RSA 密钥,并将用于对 SignedXml 对象进行签名的不对称算法密钥设置为该密钥。

```
SignedXml sig = new SignedXml(doc);
RSA m_signingKey = (RSA)new RSACryptoServiceProvider();
sig. SigningKey = signingKey;
```

2)创建一个 DataObject 对象,用以封装签名者相关信息。

```
DataObject signer =new System. Security. Cryptography. Xml. DataObject();
sig. AddObject(signer);
```

3)为签名对象添加引用,并且为该引用添加适当的变换。本研究添加了两个引用,第一个引用代表对 XML 全文进行签名(不包括签名部分的数据)。第二个引用本文只对 DataObject(包含在签名中)中的 SignerID 签名,为了从整个 XML 文档中选取某一个节点,本文应用了一个 Xpath 变换[11],将 SignerID 元素从 XML 文档中选取出来进行签名。具体如下:

```
Reference docRef = new Reference("");
docRef. AddTransform(new XmlDsigEnvelopedSignatureTransform());
Reference signerRef = new Reference("#Signer" + signerID);
stringm_xpathTransString = "<XPath xmlns:my = \" http://example
  \" >ancestor-or-self ::my:SignerID </XPath >";
XmlDsigXPathTransformxptrans = new XmlDsigXPathTransform();
xptrans. LoadInnerXml(doc. ChildNodes);
signerRef. AddTransform(xptrans);
```

4)创建一个 KeyInfo 对象,添加密钥信息:

```
KeyInfoki = new KeyInfo();
ki. AddClause(new RSAKeyValue(signingKey));
sig. KeyInfo = ki;
```

5)最后使用 ComputeSignature 方法生成 XML 签名,并以 XML 文档格式保存,完成 XML 数字签名过程。

```
sig. ComputeSignature();
```

4　结语

本文主要探讨了 XML 数字签名在工作流系统中的应用,解决了工作流系统中存在的多重签名以及对文档进行较细粒度的签名需求,提出了“签名之上的签名”的机制,给出了 XML 数字签名在工作流系统中的应用模型。基于给出的模型,将 XML 数字签名应用在一个采购审批工作流系统中,取得了较好的效果。在未来的研究中将进一步完善该模型,消除模型中可能存在的一些安全隐患。

参考文献:

[1] 张明哲,范俊逸. XML 数字签名标准与应用[J]. 电信研究,2003,32(2):299 - 306.

[2] XML-signature syntax and processing [EB/OL]. [2010 - 07 - 08]. http://www.w3. org/TR/2001/PR-xmldsig-core.

[3] Canonical XML W3C recommendation [EB/OL]. [2010 - 07 - 19]. http://www. w3. org/TR/2001/REC-xml-cl4n.

[4] 赵泽茂. 数字签名理论[M]. 北京:科学出版社,2007.

[5] 郭竞乐,赵正德,于清华,等. XML 数字签名技术的研究与实现[J]. 计算机工程与设计,2005,26(5):1211 - 1213.

[6] LEUNG K R, HUI L C. Multiple signature handling in workflow systems [C]// Proceedings of the 33rd Hawaii International Conference on System Sciences. Washington, DC: IEEE Computer Society, 2000: 6033 - 6041.

[7] 徐全生,卢丙峰. 带有图片签名的工作流技术[J]. 沈阳工业大学学报,2009,31(4):466 - 470.

[8] KUBBILUN W, CAJEK S, PSARROS M, *et al*. Trustworthy verification and visualisation of multiple XML-signatures [C]// Proceedings of the 9th IFIP TC-6 TC-11 International Conference on Communications and Multimedia Security, LNCS 3677. Berlin: Springer, 2005: 311 - 320.

[9] 蔡爽,杜平安. ERP 工作流引擎中的数字签名技术[J]. 计算机应用研究,2007,24(4):130 - 132.

[10] KITTA T. Windows workflow foundation 高级编程[M]. 陈宇寒,译. 北京:清华大学出版社,2008.

[11] XML Path Language (XPath) [EB/OL]. (1999 - 11 - 16)[2010 - 06 - 29]. http://www. w3. org/TR/Xpath.

[12] 王志晓,吕林涛,闫文耀. 基于 ASP. NET 技术和工作流模型的网上审批系统[J]. 计算机工程,2004,30(17):83 - 85.

(上接第 807 页)

4　结语

本文针对 RFID 系统安全性问题,提出了一种基于 Hash 函数和密钥阵列的安全认证协议。新协议使用标签 ID 的 Hash 函数值进一步保护标签的隐私,每一对阅读器和标签之间都拥有独立的认证密钥可进一步防止假冒攻击,可抵抗包括窃听、位置跟踪、重传攻击、拒绝服务和篡改等多种攻击方法,对抵御来自系统内部的威胁具有明显的优势。新协议的复杂程度随系统中标签和阅读器数量的增加而加大,且主要体现在服务器一端,因为在实际系统中,标签数量远远多于阅读器数量。而在计算机技术高度发达的今天,服务器技术也不应该是实现该协议的瓶颈。

随着密码学技术的不断发展,长时间使用相同密钥进行通信对该认证协议存在不安全隐患,但定时更新密钥会增加协议的复杂度,更重要的是更新密钥需确保后台服务器、阅读器和标签的密钥同步更新,一旦同步被破坏,将会给整个系统带来灾难性的影响。这将是今后研究的重点内容。

参考文献:

[1] SARMA S E, WEIS S A. Radio frequency identification: Secure risks and challenges [J]. RSA Laboratories Cryptobytes, 2003, 6(1): 2 - 9.

[2] OHKUBO M, SUZUKI K. Hash-chain based forward secure privacy protection scheme for low-cost RFID [C]// SCIS 2004: Proceedings of the 2004 Symposium on Cryptography and Information Security. Sendai: [s. n.], 2004: 719 - 724.

[3] 余恬恬,冯全源. 基于 Hash 函数的 RFID 挑战—应答认证协议[J]. 计算机工程,2009,35(24):156 - 161.

[4] 陈剑,张春,陈虹. 低功耗 RFID 的公钥密码系统实现[J]. 半导体技术,2009,34(9):890 - 894.

[5] PAISE R I, VAUDENAY S. Mutual authentication in RFID: Security and privacy [C]// Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security. New York: ACM Press, 2008: 292 - 299.

[6] 张恒山,管会生,韩海强. RFID 系统中基于公钥加密的相互认证协议[J]. 计算机工程与应用,2010,46(5):69 - 72.

[7] 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.

[8] 丁振华,李锦涛,冯波. 基于 Hash 函数的 RFID 安全认证协议研究[J]. 计算机研究与发展,2009,45(4):583 - 592.

[9] 白煜,腾建辅,张立毅,等. 基于 Hash 锁的同步强化 RFID 验证协议[J]. 计算机工程,2009,35(21):138 - 143.