(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104601334 B
(45)授权公告日 2018.09.11

(21)申请号 201510091035.5

(22)申请日 2015.03.01

(65)同一申请的已公布的文献号
申请公布号 CN 104601334 A

(43)申请公布日 2015.05.06

(73)专利权人 河北省科学院应用数学研究所
地址 050081 河北省石家庄市友谊南大街46号

(72)发明人 黎彤亮 黄世中 王怀瑞 周彦萍 王鹏 司晓琨

(74)专利代理机构 石家庄冀科专利商标事务所有限公司 13108
代理人 李羡民 高锡明

(51)Int.Cl.
*H04L 9/32*(2006.01)
*G06K 17/00*(2006.01)

(56)对比文件
CN 102737260 A,2012.10.17,
CN 102111758 A,2011.06.29,
WO 0154083 A1,2001.07.26,

审查员 许顺频

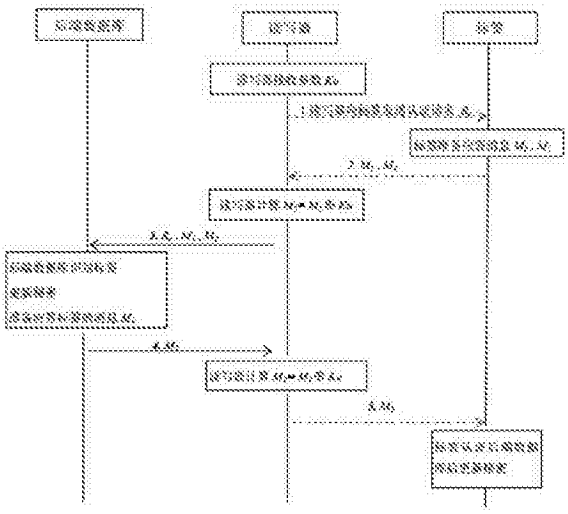
权利要求书2页 说明书5页 附图1页

(54)发明名称

一种抵抗识别表失窃的RFID双向认证方法

(57)摘要

一种抵抗识别表失窃的RFID双向认证方法，在一个执行逻辑上将RFID系统分为RFID标签、RFID读写器和后端数据库，初始时RFID标签保存其唯一标识符$ID$和密钥$T$;后端数据库除使用一个对称密码函数加密保存标签的唯一标识符$ID'$和密钥$T'$,使$ID\neq ID'$,$T\neq T'$,此外还保存标签对应识别物的信息,构成对标签的识别表,读写器读写标签时,需要接收参数$Ku$,通过这一参数和函数$E()$实现对标签的双向认证。本发明有效避免了因识别表失窃对系统产生的潜在安全隐患。



CN 104601334 B

1.一种抵抗识别表失窃的RFID双向认证方法，其特征是，所述方法在一个执行逻辑上将RFID系统分为RFID标签、RFID读写器和后端数据库、并在此系统中运行，初始时RFID标签保存其标识符ID和密钥T；后端数据库除使用一个对称密码函数加密保存标签的标识符EID和密钥ET，使ID≠EID，T≠ET；此外还保存标签对应识别物的信息，构成对标签的识别表，所述对称密码函数E()满足：$EID=E(ID)\oplus Ku$，ET＝E(T)，Ku为用户持有的参数，读写器读写标签时，需要接收参数Ku，通过这一参数和函数E()实现对标签的双向认证；具体操作按以下步骤进行：

a.初始化

后端数据库存储所管理的标签数据$<EID_i,ET_i,ET_{old_i},Info_i>$，i＝1，2，…n，n为后端数据库所管理的标签个数，$ET_{old}$，为RFID标签上一次所使用的数据，Info为RFID标签所标识物品的信息；

标签i中存储$<ID_i,T_i>$，i∈{1，2，…n}

$ID_i$，$T_i$与$EID_i$，$ET_i$的关系为：

$EID_i=E(ID_i)\oplus Ku,\quad ID_i=E^{-1}(EID_i)\oplus Ku$

$ET_i=E(T_i)$，$T_i=E^{-1}(ET_i)$

其中E()为一种加密算法，$E^{-1}()$为解密算法，所使用的密钥为dk；Ku为用户持有的一个参数；⊕为异或(XOR)运算；

b.RFID标签的识别

①使用者输入参数Ku至RFID读写器；

②RFID读写器产生一个随机数$R_r$，并将这一随机数发送给RFID标签；

③RFID标签接收到RFID读写器的读写请求后，自己产生一个随机数$R_t$，之后按下式计算应答消息$M_1$、$M_2$并将它们发送出去：

$M_1=T\oplus R_t$

$M_2=f(T\oplus R_r,\ R_t)\oplus ID$

其中，f()为另一个对称密码函数；

④RFID读写器收到RFID标签的应答消息后，使用旧所有者、或称当前所有者、卖方的参数Ku对$M_2$做如下运算：

$M_2=M_2\oplus Ku$

之后将$M_1$，$M_2$连同$R_r$发送给后端数据库进行判断；

⑤后端数据库对于所存储的每一个标签信息做如下计算：

ID'＝$E^{-1}$(EID)

T'＝$E^{-1}$(ET)

$R'_t=M_1\oplus T'$

验证：

$M_2=f(T'\oplus R_r,\ R'_t)\oplus ID'$ (1a)

是否成立；

如果不成立则计算：

$T'_{old}=E^{-1}(ET_{old})$

$R'_t = M_1 \oplus T'_{old}$

验证:

$M_2 = f(T'_{old} \oplus R_r, R'_t) \oplus ID'$ (1b)

是否成立;

如果(1a)与(1b)均不成立,则RFID标签没有通过认证,认证过程终止;

如果存在(1a)或(1b)成立,则找到标识应答标签的信息,之后准备一个消息$M_3$:

$M_3 = f(T', R'_t \oplus R_r) \oplus ID'$

随后后端数据库执行更新操作,如果(1a)成立,则更新:

$ET_{old} = ET$

无论(1a)成立还是(1b)成立,都更新:

$T_{new} = f(ID \oplus R_r, T' \oplus R'_t)$

$ET_{new} = E(T_{new})$

其中$T_{new}$、$ET_{new}$为标签下一次认证所使用的数据;

接着后端数据库将$M_3$发送给读写器;

⑥读写器计算

$M_3 = M_3 \oplus Ku$,

将$M_3$发送给RFID标签;

⑦标签验证

$M_3 = f(T, R_t \oplus R_r) \oplus ID$ ;

如果成立,则更新;

$T_{new} = f(ID \oplus R_r, T \oplus R_t)$并完成认证;

否则认证终止。

# 一种抵抗识别表失窃的RFID双向认证方法

## 技术领域

[0001] 本发明涉及一种用于RFID自动识别系统的安全双向认证方法，可防止识别表失窃给系统造成的巨大安全隐患，属于通信技术领域。

## 背景技术

[0002] 射频识别(Radio Frequency Identification-RFID)是一种利用射频信号和空间耦合(电感或电磁耦合)传输特性，实现非接触式自动识别目标对象并获取相关数据的技术。RFID技术可以提高产品的管理效率，降低管理成本，但RFID最初的应用设计是完全开放的，该技术在给系统数据采集提供灵活与方便的同时也使通过无线方式传递的信息暴露于大庭广众之下，这无疑是信息安全的重大威胁。

[0003] 一个RFID系统通常包含三个主要部分：RFID标签、RFID读写器和后端数据库。RFID标签包含唯一的标识符——ID，密钥以及一些参数，后端数据库通常保存着标签的信息和标签所标识物的信息。攻击者攻击系统，不单纯是获取标签的ID，密钥等信息，更重要的是去获得标签与标识物的对应关系。因此保护这种对应关系是保证信息安全的重要内容。

[0004] 目前，RFID系统信息安全的解决机制可以分为两个大类：一类是物理安全机制，这种安全机制主要依靠外加设备或硬件功能解决RFID系统的安全问题，如静电屏蔽、主动干扰、夹子标签等；第二类是密码机制，主要是通过基于密码技术的安全协议解决RFID系统安全问题。

[0005] 与基于物理方法的硬件安全机制相比，在电路中实现加密算法更为灵活方便，并且成本相对较低，因此基于密码技术的软件安全机制受到了人们更多的青睐，国内外诸多学者在采用基于密码技术的安全协议上做了很多工作，提出了很多方案，但已有的方案更注重保护的是标签与读写器之间的消息，而对后端服务器数据的保护关注较少，一旦后端服务器所保存的用以识别标签的识别表丢失，就会给系统所掌握的全部标签带来风险，这个风险是整体性的。同时读写器仅充当了后端服务器与标签之间通信的桥梁的作用，对读写器的使用控制缺少必要的措施。因此，现有的协议不能消除后端服务器所保存的标签信息及标签所标识物的信息失窃所带来的风险，还需要进一步研究和改进。

## 发明内容

[0006] 本发明的目的在于针对现有技术之弊端，提供一种抵抗识别表失窃的RFID双向认证方法，以解决RFID系统的信息安全问题。

[0007] 本发明所述问题是以下述技术方案实现的：

[0008] 一种抵抗识别表失窃的RFID双向认证方法，所述方法在一个执行逻辑上将RFID系统分为RFID标签、RFID读写器和后端数据库、并在此系统中运行，初始时RFID标签保存其标识符ID和密钥T；后端数据库除使用一个对称密码函数加密保存标签的标识符EID和密钥ET，使ID≠EID，T≠ET；此外还保存标签对应识别物的信息，构成对标签的识别表，所述对称密码函数E()满足：$EID=E(ID)\oplus Ku$，$ET=E(T)$，Ku为用户持有的参数，读写器读写标

签时,需要接收参数Ku,通过这一参数和函数E()实现对标签的双向认证;具体操作按以下步骤进行:

[0009] a.初始化

[0010] 后端数据库存储所管理的标签数据<$EID_i$,$ET_i$,$ET_{oldi}$,$Info_i$>,i=1,2,…n,n为后端数据库所管理的标签个数,$ET_{old}$,为RFID标签上一次所使用的数据,Info为RFID标签所标识物品的信息;

[0011] 标签i中存储<$ID_i$,$T_i$>,i∈{1,2,…n}

[0012] $ID_i$,$T_i$与$EID_i$,$ET_i$的关系为:

[0013] $$EID_i = E(ID_i) \oplus Ku, \quad ID_i = E^{-1}(EID_i) \oplus Ku$$

[0014] $ET_i = E(T_i)$,$T_i = E^{-1}(ET_i)$

[0015] 其中E()为一种加密算法,$E^{-1}$()为解密算法,所使用的密钥为dk;Ku为用户持有的一个参数;⊕为异或(XOR)运算;

[0016] b.RFID标签的识别

[0017] ①使用者输入参数Ku至RFID读写器;

[0018] ②RFID读写器产生一个随机数$R_r$,并将这一随机数发送给RFID标签;

[0019] ③RFID标签接收到RFID读写器的读写请求后,自己产生一个随机数$R_t$,之后按下式计算应答消息$M_1$、$M_2$并将它们发送出去:

[0020] $$M_1 = T \oplus R_t$$

[0021] $$M_2 = f(T \oplus R_r, R_t) \oplus ID$$

[0022] 其中,f()为另一个对称密码函数;

[0023] ④RFID读写器收到RFID标签的应答消息后,使用旧所有者、或称当前所有者、卖方的参数Ku对$M_2$做如下运算:

[0024] $$M_2 = M_2 \oplus Ku$$

[0025] 之后将$M_1$,$M_2$连同$R_r$发送给后端数据库进行判断;

[0026] ⑤后端数据库对于所存储的每一个标签信息做如下计算:

[0027] $ID' = E^{-1}(EID)$

[0028] $T' = E^{-1}(ET)$

[0029] $$R'_t = M_1 \oplus T'$$

[0030] 验证:

[0031] $$M_2 = f(T' \oplus R_r, R'_t) \oplus ID' \qquad (1a)$$

[0032] 是否成立;

[0033] 如果不成立则计算:

[0034] $T'_{old} = E^{-1}(ET_{old})$

[0035] $$R'_t = M_1 \oplus T'_{old}$$

[0036] 验证:

[0037] $$M_2 = f(T'_{old} \oplus R_r, R'_t) \oplus ID' \qquad (1b)$$

[0038] 是否成立;

[0039] 如果(1a)与(1b)均不成立,则RFID标签没有通过认证,认证过程终止;

[0040] 如果存在(1a)或(1b)成立,则找到标识应答标签的信息,之后准备一个消息$M_3$:

[0041] $M_3 = f(T', R'_t \oplus R_r) \oplus ID'$

[0042] 随后后端数据库执行更新操作,如果(1a)成立,则更新:

[0043] $ET_{old} = ET$

[0044] 无论(1a)成立还是(1b)成立,都更新:

[0045] $T_{new} = f(ID \oplus R_r, T' \oplus R'_t)$

[0046] $ET_{new} = E(T_{new})$

[0047] 其中$T_{new}$、$ET_{new}$为标签下一次认证所使用的数据;

[0048] 接着后端数据库将$M_3$发送给读写器;

[0049] ⑥读写器计算

[0050] $M_3 = M_3 \oplus Ku$,

[0051] 将$M_3$发送给RFID标签;

[0052] ⑦标签验证

[0053] $M_3 = f(T, R_t \oplus R_r) \oplus ID$ ;

[0054] 如果成立,则更新;

[0055] $T_{new} = f(ID \oplus R_r, T \oplus R_t)$并完成认证;

[0056] 否则认证终止。

[0057] 本发明对识别表设置了双层保护,一是对识别表进行加密;二是通过设置参数切断识别表中所保存的数据与标签所保存数据的直接对应关系,这样就有效避免了因识别表失窃对系统产生的巨大潜在安全隐患。

## 附图说明

[0058] 下面结合附图对本发明作进一步说明。

[0059] 图1是本发明的数据处理流程图。

[0060] 图中各符号为:$M_1$,$M_2$,$M_3$为消息,$\overrightarrow{MSG}$为可信的消息,$\overrightarrow{MSG}$为不可信的消息,⊕为异或运算。

[0061] 文中各符号为:Ku为用户持有的参数,ID为RFID标签的唯一标识符,ET为RFID标签的密钥,$ID_i$为第i个RFID标签的唯一标识符,$T_i$为第i个RFID标签的密钥,Info为标签所标识物品的信息,E()为一种加密算法,$E^{-1}$()为解密算法,其密钥为dk,在后端服务器中安全保存并使用,$R_r$为RFID读写器产生的一个向标签发起查询的数,$R_t$为RFID标签产生一个随机数,f()为一个对称密码函数。

## 具体实施方式

[0062] 本发明提出一种RFID标签和读写器之间的双向认证方法,相对于其他方法,本方法可以防止因后端服务器所保持的标签信息及标签所标识物的信息失窃所带来的风险。

[0063] 具体步骤包括:

[0064] 1.初始化

[0065] 后端数据库存储所管理的标签数据<$EID_i$,$ET_i$,$ET_{oldi}$,$Info_i$>,i=1,2,…n,n为后

端数据库所管理的标签个数,$ET_{old}$,为标签上一次所使用的数据,Info为标签所标识物品的信息。

[0066] 标签i中存储<$ID_i$,$T_i$>,i∈{1,2,…n}

[0067] $ID_i$,$T_i$的与$EID_i$,$ET_i$关系为:

[0068] $$EID_i = E(ID_i) \oplus Ku,\ ID_i = E^{-1}(EID_i) \oplus Ku$$

[0069] $ET_i = E(T_i)$,$T_i = E^{-1}(ET_i)$

[0070] 读写器连接后端服务器时需要进行安全认证等工作,建立起可信的消息传递的安全通道。

[0071] 2.识别

[0072] 步骤0:运行前准备。使用者输入参数Ku至读写器。

[0073] 步骤1:RFID读写器将一任意数$R_r$发送给RFID标签。

[0074] 步骤2:标签接收到读写器的读写请求后,自己产生一个随机数$R_t$,之后计算应答消息$M_1$,$M_2$并将它们发送出去:

[0075] $$M_1 = ET \oplus R_t$$

[0076] $$M_2 = f(ET \oplus R_r, R_t) \oplus ID$$

[0077] 步骤3:读写器收到标签的应答的消息后,使用参数Ku对$M_2$做如下运算:

[0078] $$M_2 = M_2 \oplus Ku$$

[0079] 之后将$M_1$,$M_2$连同$R_r$发送给后端数据库进行判断。

[0080] 步骤4:后端数据库对于所存储的每一个标签信息做如下计算:

[0081] $EID = E^{-1}(EID)$

[0082] $T' = E^{-1}(ET)$

[0083] $$R_t' = M_1 \oplus T$$

[0084] 验证:

[0085] $$M_2 = f(T' \oplus R_r, R_t') \oplus ID \qquad (1a)$$

[0086] 是否成立。

[0087] 如果不成立则计算:

[0088] $T'_{old} = E^{-1}(ET_{old})$

[0089] $$R_t' = M_1 \oplus T_{old}$$

[0090] 验证:

[0091] $$M_2 = f(T'_{old} \oplus R_r, R_t') \oplus ID \qquad (1b)$$

[0092] 是否成立。

[0093] 如果(1a)与(1b)均不成立,则RFID标签没有通过认证,认证过程终止;

[0094] 如果存在(1a)或(1b)成立,则表示后端数据库找到标识应答标签的信息,之后准备一个消息$M_3$:

[0095] $$M_3 = f(T', R'_t \oplus R_r) \oplus EID$$

[0096] 随后后端数据库执行更新操作,如果(1a)成立,则更新:

[0097] $ET_{old} = ET$

[0098] 无论(1a)成立还是(1b)成立,都更新:

[0099] $T_{new}=f(ID\oplus R_r, T'\oplus R'_t)$

[0100] $ET_{new}=E(T_{new})$

[0101] 接着后端数据库将$M_3$发送给读写器。

[0102] 步骤5:读写器计算

[0103] $M_3=M_3\oplus Ku$

[0104] 将$M_3$发送给标签。

[0105] 步骤6:标签验证

[0106] $M_3=f(ET, R_t\oplus R_r)\oplus ID$

[0107] 如果成立,则更新

[0108] $T_{new}=f(ID\oplus R_r, T\oplus R_t)$

[0109] 并完成过程;否则过程终止。

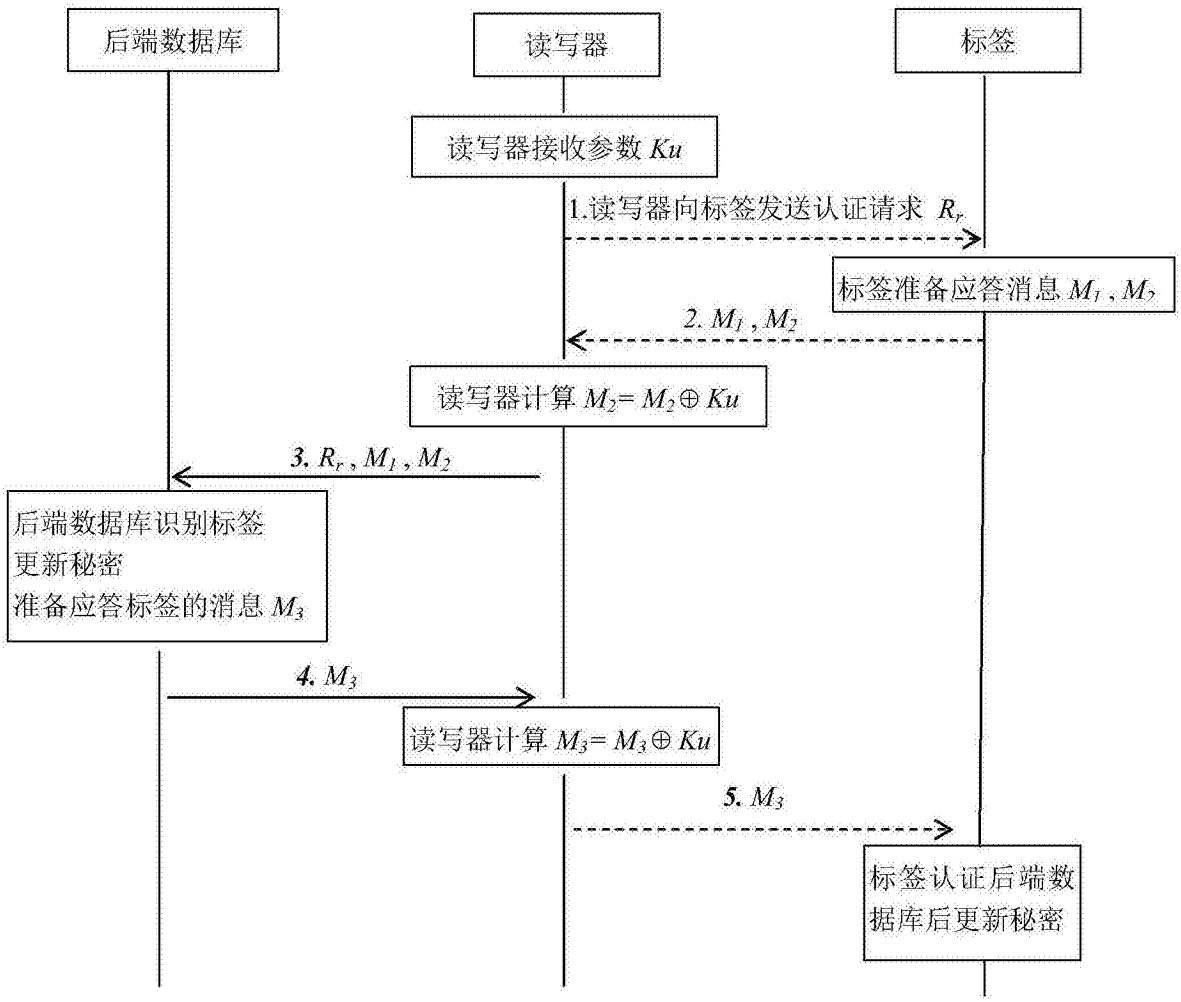

后端数据库
读写器
标签
读写器接收参数 Ku
1.读写器向标签发送认证请求 $R_r$
标签准备应答消息 $M_1$ , $M_2$
2. $M_1$ , $M_2$
读写器计算 $M_2$= $M_2$⊕ Ku
3. $R_r$ , $M_1$ , $M_2$
后端数据库识别标签
更新秘密
准备应答标签的消息 $M_3$
4. $M_3$
读写器计算 $M_3$= $M_3$⊕ Ku
5. $M_3$
标签认证后端数据库后更新秘密

图1