单个 RFID 所有权转移协议的设计和安全性分析

桂易琪[1],张　杰[2]

(1.扬州大学信息工程学院,江苏 扬州 225009)
(2.河海大学物联网工程学院,江苏 南京 210098)

[**摘要**]　虽然现有的 RFID 安全协议的地址标签验证问题很重要,但是这些标签的主体转移所有权的能力也相当重要. 近年来,一些轻量级的加密认证协议被提出来解决这个问题,然而他们大多数假定 RFID 的读写器 reader 和后端系统 DB 服务器之间通信安全却忽略了反向的不可追溯性. 我们考虑一些 RFID 所有权转移的突变,并提出单一认证的 RFID 所有权转移协议,该协议是轻量级的,安全的,同时协议实现了标签和数据库服务器之间相互认证. 此外,我们在 BAN 逻辑和串空间的基础上提供安全分析来评估和论证了该协议的准确性.

[**关键词**]　RFID,所有权转移,BAN 逻辑,串空间.
[**中图分类号**]TP393.08　[**文献标志码**]A　[**文章编号**]1672-1292(2015)02-0065-08

Design and Analysis of Single RFID Ownership Transfer Protocol

Gui Yiqi[1],Zhang Jie[2]

(1.Department of Information Engineering,Yangzhou University,Yangzhou 225009,China)
(2.Department of IOT Engineering,Hohai University,Nanjing 210098,China)

Abstract:While the major existing RFID security protocols address tag authentication issues,the ability of transferring ownership of these tagged objects is most equally important. Recently,though some lightweight encrypted authentication protocols have been proposed to solve the problem,most of them assume that the channel between the RFID reader and the DB sever is so secure that the backward un-traceability is ignored. We consider a few RFID ownership transfer mutations and propose a single authentication RFID ownership transfer protocol that is lightweight and secure. Due to challenge response mechanism,the protocol achieves mutual authentication between tag and DB server. Also,we provide security analysis to evaluate and proof the accuracy based on BAN logic and strand space. The merit of our protocol achieves high-security and high-efficiency.

Key words:RFID,ownership transfer,BAN logic,strand space

目前,无线射频识别(RFID)技术[1-9],在社会上得到了广泛的欢迎和重视. 这些应用程序(如反恐、进出口管理等)的主要性需要这些 RFID 标记的对象随着时间的推移由不同的实体拥有. 这需要一个标记对象的严谨的所有权转移机制的存在. RFID 标签的所有权必须在其使用期中经常地更改,以保护链中每个点的信息和隐私. 所有权转移必须保证,一旦所有权转移给另一实体,新的所有者和前所有者的信息和隐私都应该得到保护. 因此,在 RFID 系统中所有权转移标签认证应主要考虑以下安全要求[4,8,10]:

- 抗重传攻击:重传攻击是网络攻击的一种形式,它将有效的数据传输恶意或欺诈性地重复或延迟.
- 信息泄漏:标签可以存储用户的隐私信息,如姓名、年龄、位置等. 信息不能泄露以及有相应的权限.
- 不可回溯性:存储在标签中的位置隐私可能被攻击者用来追踪标签的所有者. 此外,一些其他信息也可以用来跟踪,例如,一个没有任何更新计划的假名.
- 前向和后向的安全性:前向/后向的安全性是指一个攻击者即使获得现在的(早先的)机密信息,也不会破解早先的(现在的)机密信息.

收稿日期:2014-08-20.
基金项目:江苏省扬州市扬州大学科研启动基金(0374780015632).
通讯联系人:桂易琪,博士,讲师,研究方向:信息安全以及流媒体通信,数据挖掘的研究. E-mail:yqgui@yzu.edu.cn

• 抗服务(DoS)攻击:攻击者可能通过更新秘密阻止合法的标签,导致服务器和标签去同步化. 合法的标签不能再获得服务器的认证.

• 所有权转移:所有权转移要求,即使当前的所有者把必要的数据传给新所有者,入侵当前的和新所有者的隐私的事件也不会发生.

本文中,我们提出了一个轻量级协议,满足 RFID 系统中的安全性要求. 我们提出的协议的优点是它不仅能满足前向/后向安全,而且也提供了读-写器身份验证和相互身份验证. 本文的结构如下:下一节对以前的一些所有权转移的标签认证中存在固有缺陷的协议做了简要概述. 第 3 节提出了我们的安全协议和分析提出的解决方案的安全性. 最后,我们将在第 4 节总结本文.

1　对早先协议的分析

首先,我们提供了一些相关协议的概述. 我们从散列函数和对称密钥密码系统开始考虑. 我们假定消息的发起者等待预先规定的时间内的响应,无响应则触发新的消息.

1.1　符号

表 1　给出在本文中使用的相关符号

Table 1　Present the notations used in this paper

Info(TID)	标签的相关信息
f	对称密钥加密功能
f'_k,f_k	键控(用密钥 k)加密功能
h,H,	散列函数-$\{0,1\}^*(\{0,1\}^1$(或$\{0,1\}^k$)
h_k	键控(用密钥 k)的散列函数
R_i,T_i	读写器 i,标签 i
TID,RID	标签和读写器的标识符
k,k',k''	认证密钥
Nj	由实体 j 生成的 1 位随机数
OT	所有权转移
TTP	受信任的第三方
$\oplus$, $\|$	异或,连接运算符

1.2　回顾和分析以前的协议

为了处理 RFID 系统的安全问题,研究人员提出了几种不同的方法. 早期低消耗的方法应该是 Osaka 的方法[1]. Osaka 的方法存在一些问题. 首先,攻击可以拦截从读写器到标签的第一个消息,并发送在同一个 N_R 给标签. 由于标签的响应 $H(f_k(ID)\oplus N_R)$ 仅由 $f_k(ID)$ 和攻击者的 N_R 计算得来的. 因此攻击(更改 $N_R=0$)将接收相同的响应 $H(f_k(ID))$. 这可以被用来跟踪标签. 在 Osaka 的协议中,一旦标签的秘密数据 $f_{k'}(ID)$ 被泄露,以前所有的秘密数据 $f_k(ID)$ 也将被破解,因此,以往的通信信息也将被公开. 假设一个标签被破解,那么攻击者会得到标签的值 $f_{k'}(ID)$. 从过去通信中窃听的数据(e,a,N_R),攻击者可以通过执行下列检查步骤来验证通信是否来自相同的标签:因为 $e\oplus f_{k'}(ID)$ 等于 $f_k(ID)$:$e\oplus f_{k'}(ID)=f_k(ID)\oplus f_{k'}(ID)\oplus f_{k'}(ID)$,所以攻击者计算 $e\oplus f_{k'}(ID)$ 得出值 $f_k(ID)$. 攻击者可以通过使用上述攻击方法跟踪一个被破解的标签的过去的所有通信. Osaka 的方法不能抵抗拒绝服务攻击,攻击者可以很容易地使数据库拒绝来自标签的任何身份验证请求. 首先,作者没有说明标签是如何可以从包含为了更新新的 $f_{k'}(ID)$ 的数据的消息中区分出传入的包含随机数 N_R 的读消息. 如果这些信息不能分离,那么标签可能会把随机 N_R 混淆为更新的新 $f_{k'}(ID)$. 新的 $f_{k'}(ID)$ 将是 $N_R\oplus f_{k'}(ID)$,导致标签实际无效. 类似地,因为写信息的完整性未经验证,在传输过程中单比特的错误可以杀死标签,那么新的 $f_{k'}(ID)$ 将是未知的. 因此,攻击者可以伪造读,然后发送随机的数据作为写入的消息,这将导致有效的新的 $f_{k'}(ID)$ 变成无效的.

一些作者[4-8]曾试图改善这一协议. 例如,Jappinen 和 Hamalainen 使用两个值,$m1=f_k(ID)\oplus f_{k'}(ID)$,$m2=H(f_k(ID)\oplus N_D$ 提供前向安全性和防 DoS 攻击的安全性,其中 N_D 是 1 个由数据库生成的随机数. 但是我们可以看到,$m1$ 与 e 是相同的,因此该方法不能提供前向安全性. 由于在读写器和标签之间的信道是不安全的,标签接收到的最后的消息 $m1$,$m2$ 可能不正确(它可能是攻击者或是通道中的噪声引起的),但数据库也无法确认标签中 k 和 $f_k(ID)$ 的更新. 这导致去同步化,因此标签和读写器/数据库之间引起 DoS

攻击问题.

Lei 和 Cao 也修改了 Osaka 协议,以避免可追溯性和 DoS 攻击. 然而,这个协议还存在多个漏洞. 该协议的 1 个漏洞是明确地验证读写器身份的失败. 攻击者可以冒充诚实的读写器,发送(Query,N_R)给标签,得到回复(N_T,$H(f_k(ID))\oplus N_R \| N_T$)). 然后攻击者转发($N_R$,$N_T$,$H(f_k(ID))\oplus N_R \| N_T$))到数据库中,这共享标签的信息和攻击者的 $Info(ID)$. 该协议将导致假读写器的安全问题. 此外,这是 1 个所有权分享协议而非所有权转移(而不是 OT)协议,因为以前的所有者可以保持标签的射频(RF)所有权. 当新的所有者获得 1 个新的密钥(k')时,它在信道中向标签发送(e,m)是不安全的. 前所有者捕捉到从读写器到标签的 $e=H(f_k(ID))\oplus f_{k'}(ID)$时,$f_{k'}(ID)$可以由 $H(f_k(ID))$和 e 得到. 前所有者通过这些信息可以冒充标签与读写器/数据库通信. 因为标签直到下一个 OT 才使用$f_{k'}(ID)$,所以前所有者拥有标签的持久所有权.

Song[9] 提出了 1 种没有 TTP 的 RFID 标签所有权转移协议. 这个协议包括两个阶段. 第一阶段是所有者 $R1$ 转移所有权到另一个所有者 $R2$,第二阶段是更新秘密. 新的所有者通过发送一个随机数给标签,标签产生另一个随机数并发送相关消息以启动这些过程. 然后新的所有者联系以前的合法验证信息和共享标签信息的所有者. 现在,这两个(新的和以前的)所有者知道标签的秘密. 新的所有者生成 1 组新的秘密并与标签分享它们. 新的所有者在消息被成功验证后更新密钥. 标签和新的所有者之间去同步化是另一个安全问题. OT 协议中,它表现为 $R2$ 有新的密钥,而标签在攻击者阻碍 $R2$ 和标签之间的最后通信时仍有以前的密钥.

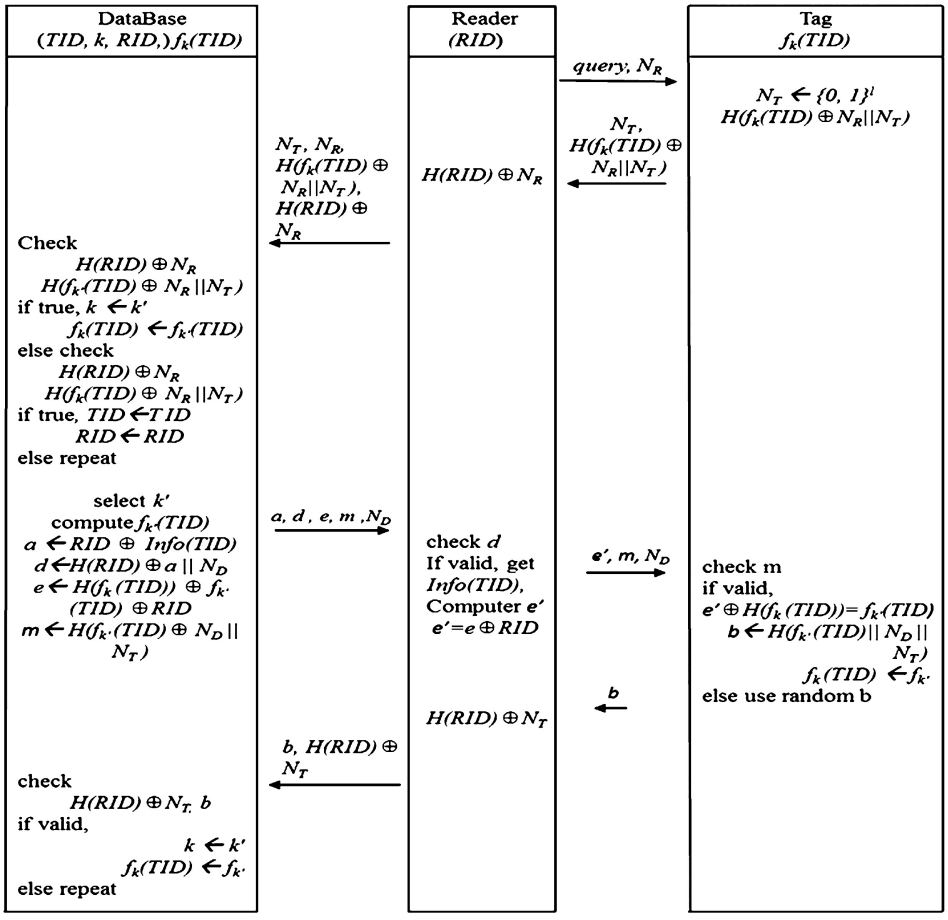

图 1　OT 协议的认证过程

Fig. 1　Authencation process with OT

2　设计和分析 OT 协议

现在,我们提出协议来实现标签和后端数据库之间的相互认证,并且还旨在提供抵抗伪读写器的安全问题. 本协议的目的是为了满足所有权转移时所有者的隐私和安全要求. 如现有的 OT 协议,我们假设标

签是低成本的无源标签,并且轻量级的功能是存在的. 读写器与标签和后端数据库之间的通信是经由不安全的通道. 因此攻击者可以通过协议拦截和篡改所有消息. 为了防止 DoS 攻击,以明文发送的新产生的随机数的接收者(如图 1,N_D 从后端数据库发送给标签)仅当此随机数不为空时才接受它. 我们假定消息的发起者等待预先规定的时间内的响应,无响应则触发新的消息.

2.1　身份验证过程

(1)读写器广播疑问和随机数 N_R 给标签.

(2)标签生成 1 个随机数 N_T,然后计算 $H(f_k(TID)\oplus N_R\parallel N_T)$并发送到读写器.

(3)读写器计算 $H(RID)\oplus N_R$,然后转发 $H(f_k(TID)\oplus N_R\parallel N_T)$,$H(RID)\oplus N_R$,$N_T$,$N_R$ 到数据库.

(4)数据库首先试图找到 RID、$f_k(TID)$、$H(f_k(TID)\oplus N_R\parallel N_T)$,然后数据库计算出 $H(RID)\oplus N_R$,并比较是否等同于接收到的来自读写器的 $H(RID)\oplus N_R$. 数据库获得 TID 和 RID.

(5)首先数据库查找 $Info(TID)$,然后数据库生成新的对称密钥 k'和一个随机数 N_D. 计算并发送 a、d、e、m、N_D 到读写器.

(6)读写器检查 $d=H(RID)\oplus a\parallel N_D$,得到必要的信息 $Info(TID)$,然后计算 e',并发送 e'、m、N_D 到标签.

(7)首先由 $e'\oplus H(f_k(TID))$计算出$f_{k'}(TID)$,其次更新其保存的数据$f_k(TID)$为$f_{k'}(TID)$,然后标签检查 m. 如果 m 是有效的,标签计算变量 $b=H(f_{k'}(TID)\parallel N_D\parallel N_T)$并发送到读写器;若 m 是无效的,标签产生 1 个随机 b 并发送到读写器.

(8)读写器计算 $H(RID)\oplus N_T$,然后转发 b、$H(RID)\oplus N_T$ 到数据库.

(9)检查读写器的身份验证,计算 b. 若 b 是有效的,数据库更新密钥 k'、$f_{k'}(TID)$,认证过程结束. 若 b 是无效的,转到步骤 1. 当重复认证过程时,数据库应该在步骤 3 计算另一个值 $H(f_{k'}(TID)\oplus N_R\parallel N_T)$. 如果值是有效的,数据库更新密钥 k'、$f_{k'}(TID)$,然后认证过程结束.

2.2　安全分析

本节中,我们给我们提出的协议进行简要的安全分析.

前向/后向的安全性:即使现在的$f_{k'}(TID)$泄露出去,TID 和$f_k(TID)$也不会泄露给不知道对称密钥 k 的攻击者. 而攻击者通过计算 $e'\oplus H(f_{k'}(TID))$无法获得$f_k(TID)$,他得到是 $H(f_k(TID))$. 因为不可能解密 H,知道 $H(f_k(TID))$对攻击者来说没有优势,他也不能得到$f_k(TID)$. 因此,我们的计划实现了前向安全性. 同样的道理,它实现了后向安全性.

抗重传攻击:由合法读写器和标签发送 N_R、N_T 不同于窃听到的 N'_R、N'_T. 因此 $H(f_k(TID)\oplus N_R\parallel N_T)$和 $H(f_k(TID)\oplus N'_R\parallel N'_T)$由于散列函数的冲突抵抗性能也不同. 因此攻击者不能伪装成合法的标签,$N_R\neq N'_R$ 且 $N_T\neq N'_T$因为

$$H(f_k(TID)\oplus N_R\parallel N_T)\mid H(f_k(TID)\oplus N'_R\parallel N'_T)$$

可追溯性:攻击者使用标签发送的同样的消息来跟踪标签位置. 攻击者无法追踪标签位置的原因如下:攻击者拦截 1 s 和 n s 的通讯消息:$msg1$、$msg1'$,但不能保证 $msg1$ 和 $msg1'$从相同的标签发送. 原因说明如下:

$$msg1=H(f_k(TID)\oplus N_R\parallel N_T),\quad msg1'=H(f_{k'}(TID)\oplus N'_R\parallel N'_T)$$

由于随机数 N_R、N_T 和密钥 k 各自的处理不同,我们的协议可以抵抗跟踪攻击.

信息泄漏:攻击者无法伪装成 1 个合法的读写器,以获得标签的信息. 数据库接收并验证它,如下所示:接收到的 $H(RID)\oplus N_R$ 是否等于数据库计算得到的 $H(RID)\oplus N_R$

若成立,则读写器合法. 否则,数据库将终止认证处理.

所有权可转移性:提出的协议能够转移所有权而不存在通过更改由 ID 加密的对称密钥 k 对新所有者的隐私的入侵. 因此,提出的协议实现了所有权转移.

2.3　正确性的形式化证明

我们现在使用 BAN 逻辑[3]验证消息源假设的正确性,BAN 逻辑不仅能发现加密协议的当前各种攻击,而且能全面地找出缺陷. 我们找到协议中的个人信息,紧跟着是内在的明确的假设,接着是目标. 然后我们使用 BAN 逻辑证明这些目标.

协议信息:

$$M1:\text{Reader}\rightarrow\text{DB}:\{N_R,N_T,f_k(TID),\text{DB}\xleftrightarrow{f_k(TID)}\text{T}\}_{f_k(TID)},\{N_R,RID,\text{DB}\xleftrightarrow{RID}R\}_{RID}$$

$$M2:\text{DB}\rightarrow\text{Reader}:\{N_D,RID,H(f_k(TID)\oplus f_{k'}(TID)),\text{DB}\xleftrightarrow{RID}R\}_{RID}$$

$$M3:\text{Reader}\rightarrow\text{Tag}:\{N_D,f_k(TID),f_{k'}(TID),\text{DB}\xleftrightarrow{f_k(TID)}\text{T}\}_{f_k(TID)}$$

$$M4:\text{Tag}\rightarrow\text{DB}:\{N_T,RID\}_{RID},\{N_T,f_{k'}(TID),\text{DB}\xleftrightarrow{f_{k'}(TID)}\text{T}\}_{f_{k'}(TID)}$$

假设:

$$A1:\text{T}|\equiv\text{T}\xleftrightarrow{f_k(TID)}\text{DB}\qquad A2:\text{DB}|\equiv\text{DB}\xleftrightarrow{f_k(TID)}\text{T}$$

$$A3:\text{R}|\equiv\text{R}\xleftrightarrow{RID}\text{DB}\qquad A4:\text{DB}|\equiv\text{DB}\xleftrightarrow{RID}\text{R}$$

$$A5:\text{T}|\equiv\#(N_T,N_R,N_D)\qquad A6:\text{R}|\equiv\#(N_T,N_R,N_D)$$

$$A7:\text{DB}|\equiv\#(N_T,N_R,N_D)\qquad A8:\text{DB}|\equiv T|\Rightarrow f_k(TID)$$

$$A9:\text{T}|\equiv\text{DB}|\Rightarrow f_k(TID)\qquad A10:\text{T}|\equiv\text{DB}|\Rightarrow f_{k'}(TID)$$

$$A11:\text{DB}|\equiv\text{T}|\Rightarrow f_{k'}(TID)\qquad A12:\text{DB}|\equiv\text{DB}\xleftrightarrow{f_{k'}(TID)}\text{T}$$

目标的正确证明:提出的协议的首要目标是信念(|≡),及每一个 DB 服务器、读写器、标签之间的信息的新鲜度(#). 信念可以确保消息是来自可信来源. 新鲜性确保消息在同一会话中早些时候不会被发送.

目标:

$$G1:\text{DB}|\equiv\text{T}|\equiv\text{DB}\xleftrightarrow{f_k(TID)}\text{T}\qquad G2:\text{T}|\equiv\text{DB}|\equiv\text{DB}\xleftrightarrow{f_k(TID)}\text{T}$$

$$G3:\text{DB}|\equiv\text{R}|\equiv\text{DB}\xleftrightarrow{RID}\text{R}\qquad G4:\text{R}|\equiv\text{DB}|\equiv\text{DB}\xleftrightarrow{RID}\text{R}$$

$$G5:\text{DB}|\equiv f_k(TID)\qquad G6:\text{T}|\equiv f_k(TID)$$

$$G7:\text{DB}|\equiv f_{k'}(TID)\qquad G8:\text{T}|\equiv f_{k'}(TID)$$

证明 下面提到的逻辑假定数字(如 M1. P1…)来自参考文献[4]:

$$[\text{D1}:]\ \text{DB}\lhd\{N_R,N_T,f_k(TID),\text{DB}\xleftrightarrow{f_k(TID)}\text{T}\}_{f_k(TID)},\{N_R,RID,\text{DB}\xleftrightarrow{RID}\text{R}\}_{RID}\quad /*\text{M1}*/$$

$$[\text{D2}:]\ \text{DB}\lhd\{N_R,N_T,f_k(TID),\text{DB}\xleftrightarrow{f_k(TID)}\text{T}\}_{f_k(TID)}\quad /*\text{D1,P7}*/$$

$$[\text{D3}:]\ \text{DB}|\equiv\text{T}|\sim\{N_R,N_T,f_k(TID),\text{DB}\xleftrightarrow{f_k(TID)}\text{T}\}\quad /*\text{D2,A2,P1}*/$$

$$[\text{D4}:]\ \text{DB}|\equiv\#\{N_R,N_T,f_k(TID),\text{DB}\xleftrightarrow{f_k(TID)}\text{T}\}\quad /*\text{A7,P6}*/$$

$$[\text{D5}:]\ \text{DB}|\equiv\text{T}|\equiv\{N_R,N_T,f_k(TID),\text{DB}\xleftrightarrow{f_k(TID)}\text{T}\}\quad /*\text{D3、4,P2}*/$$

$$[\text{D6}:]\ \text{DB}|\equiv\text{T}|\equiv\text{DB}\xleftrightarrow{f_k(TID)}\text{T}\quad /*\text{D5,P5}*/$$

$$[\text{D7}:]\ \text{DB}|\equiv\text{T}|\equiv f_k(TID)\quad /*\text{D5,P5}*/$$

$$[\text{D8}:]\ \text{DB}|\equiv f_k(TID)\quad /*\text{D7,A8,P3}*/$$

$$[\text{D9}:]\ \text{DB}\lhd\{N_R,RID,\text{DB}\xleftrightarrow{RID}\text{R}\}_{RID}\quad /*\text{D1,P7}*/$$

$$[\text{D10}:]\ \text{DB}|\equiv\text{R}|\sim\{N_R,RID,\text{DB}\xleftrightarrow{RID}\text{R}\}\quad /*\text{D9,A4,P1}*/$$

$$[\text{D11}:]\ \text{DB}|\equiv\#\{N_R,RID,\text{DB}\xleftrightarrow{RID}\text{R}\}\quad /*\text{A6,P6}*/$$

$$[\text{D12}:]\ \text{DB}|\equiv\text{R}|\equiv\{N_R,RID,\text{DB}\xleftrightarrow{(RID)}\text{R}\}\quad /*\text{D10、11,P2}*/$$

$$[\text{D13}:]\ \text{DB}|\equiv\text{R}|\equiv\text{DB}\xleftrightarrow{(RID)}\text{R}\quad /*\text{D12,P5}*/$$

$$[\text{D14}:]\ \text{R}\lhd\{N_D,RID,H(f_k(TID)\oplus f_{k'}(TID)),\text{DB}\xleftrightarrow{(RID)}\text{R}\}_{RID}\quad /*\text{M2}*/$$

$$[\text{D15}:]\ \text{R}|\equiv\text{DB}|\sim\{N_D,RID,H(f_k(TID)\oplus f_{k'}(TID)),\text{DB}\xleftrightarrow{(RID)}\text{R}\}\quad /*\text{D14,P1,A3}*/$$

$[\mathrm{D16}:]\mathrm{R}\mid\equiv\#\{N_D,RID,H(f_k(TID)\oplus f_{k'}(TID)),\mathrm{DB}\overset{(RID)}{\longleftrightarrow}\mathrm{R}\}$　　/ * A6,P6 * /

$[\mathrm{D17}:]\mathrm{R}\mid\equiv\mathrm{DB}\mid\equiv\{N_D,RID,H(f_k(TID)\oplus f_{k'}(TID)),\mathrm{DB}\overset{(RID)}{\longleftrightarrow}\mathrm{R}\}$　　/ * D15、16,P2 * /

$[\mathrm{D18}:]\mathrm{R}\mid\equiv\mathrm{DB}\mid\equiv\mathrm{DB}\overset{(RID)}{\longleftrightarrow}\mathrm{R}$　　/ * D17,P5 * /

$[\mathrm{D19}:]\mathrm{T}\lhd\{N_D,f_k(TID),f_{k'}(TID),\mathrm{DB}\overset{f_k(TID)}{\longleftrightarrow}\mathrm{T}\}_{f_k(TID)}$　　/ * M3 * /

$[\mathrm{D20}:]\mathrm{T}\mid\equiv\mathrm{DB}\mid\sim\{N_D,f_k(TID),f_{k'}(TID),\mathrm{DB}\overset{f_k(TID)}{\longleftrightarrow}\mathrm{T}\}$　　/ * D19,A1,P1 * /

$[\mathrm{D21}:]\mathrm{T}\mid\equiv\#\{N_D,f_k(TID),f_{k'}(TID),\mathrm{DB}\overset{f_k(TID)}{\longleftrightarrow}\mathrm{T}\}$　　/ * A5,P6 * /

$[\mathrm{D22}:]\mathrm{T}\mid\equiv\mathrm{DB}\mid\equiv\{N_D,f_k(TID),f_{k'}(TID),\mathrm{DB}\overset{f_k(TID)}{\longleftrightarrow}\mathrm{T}\}$　　/ * D20、21,P2 * /

$[\mathrm{D23}:]\mathrm{T}\mid\equiv\mathrm{DB}\mid\equiv\mathrm{DB}\overset{f_k(TID)}{\longleftrightarrow}\mathrm{T}$　　/ * D22,P5 * /

$[\mathrm{D24}:]\mathrm{T}\mid\equiv f_k(TID)$　　/ * D22,A9,P3 * /

$[\mathrm{D25}:]\mathrm{T}\mid\equiv f_{k'}(TID)$　　/ * D22,A10,P3 * /

$[\mathrm{D26}:]\mathrm{DB}\lhd\{N_T,RID\}_{RID},\{N_T,f_{k'}(TID),\mathrm{DB}\overset{f_{k'}(TID)}{\longleftrightarrow}\mathrm{T}\}_{f_{k'}(TID)}$　　/ * M4 * /

$[\mathrm{D27}:]\mathrm{DB}\lhd\{N_T,f_{k'}(TID),\mathrm{DB}\overset{f_{k'}(TID)}{\longleftrightarrow}\mathrm{T}\}_{f_{k'}(TID)}$　　/ * D26 * /

$[\mathrm{D28}:]\mathrm{DB}\mid\equiv\mathrm{T}\mid\sim\{N_T,f_{k'}(TID),\mathrm{DB}\overset{f_{k'}(TID)}{\longleftrightarrow}\mathrm{T}\}$　　/ * D27,A12,P1 * /

$[\mathrm{D29}:]\mathrm{DB}\mid\equiv\#\{N_T,f_{k'}(TID),\mathrm{DB}\overset{f_{k'}(TID)}{\longleftrightarrow}\mathrm{T}\}$　　/ * A7,P6 * /

$[\mathrm{D30}:]\mathrm{DB}\mid\equiv\mathrm{T}\mid\equiv\{N_T,f_{k'}(TID),\mathrm{DB}\overset{f_{k'}(TID)}{\longleftrightarrow}\mathrm{T}\}$　　/ * D28、29,P2 * /

$[\mathrm{D31}:]\mathrm{DB}\mid\equiv\mathrm{T}\mid\equiv f_{k'}(TID)$　　/ * D30,P5 * /

$[\mathrm{D32}:]\mathrm{DB}\mid\equiv f_{k'}(TID)$　　/ * D31,A11,P3 * /

如上显示,目标的证明分别在步骤 D6、D23、D13、D18、D8、D24、D32 和 D25 实现.

BAN 逻辑区分 1 个主体可以拥有什么以及它可以相信什么. 它能表达不同信任级别和协议步骤背后隐含的条件. 但是 BAN 无法解决各个实体(DB 服务器,读写器,标签)所获悉其禁止的事实. 我们考虑上述情况可能违反了本文已经提到 RFID 的安全要求,可是显示了该协议下考虑到的威胁是安全的. 因此,我们现在使用串空间[2]证明该协议这种情况下的正确性.

为了用串空间证明,我们使用下面的符号.

(1)P、Σ:攻击者串空间、串空间;

(2)T、T_{name}:设置相当于原子消息的文本;

(3)C:簇;

(4)K_p:攻击者知道的密钥集合;

(5)$\prec$:优先关系;

(6)$\subset$:包含于.

定义 1　一个攻击者串空间 P,Σ 是 P_{OT}串空间. 假设 Σ 是下面 3 种串空间的集合.

(1)攻击者串 $p\in P$.

(2)发起者串 Init[DB,Tag,N_D,N_T],其迹为

$$\langle +N_D,H(f_k(TID))\oplus f_{k'}(TID),H(f_{k'}(TID)\oplus N_D\parallel N_T),-H(f_{k'}(TID)\parallel N_D\parallel N_T)\rangle$$

式中:DB,Tag $\in T_{\mathrm{name}}$,但 $N_D\notin T_{\mathrm{name}}$.

(3)响应者串 Resp[DB,Tag,N_D,N_T],其迹为

$$\langle -N_D,H(f_k(TID))\oplus f_{k'}(TID),H(f_{k'}(TID)\oplus N_D\parallel N_T),+H(f_{k'}(TID)\parallel N_D\parallel N_T)\rangle$$

2.3.1　认证属性的证明

命题 1　假设

(1)Σ 是 P_{OT}串空间,C 是包含发起者串 $s\in$ Init[DB,Tag,N_D,N_T]的簇;

(2)$k \notin K_p$;

(3)$N_D \neq N_T$,N_D 唯一起源于 Σ;那么 C 包含 1 个响应者串 $t \in \text{Resp}[\text{DB},\text{Tag},N_D,N_T]$.

引理 1 起源于第一个消息(来自于 DB).

我们知道 $H(f_k(TID)) \oplus f_{k'}(TID)$ 和 $N_D \in \text{DB}$(称作,n_0)来自第一个消息(称作 v_0)是正节点且起源于 DB. 所以我们需要证实不出现该串之前的节点(这里,Tag). 由定义,这些都是真的.

引理 2 集合 $S=\{n \in C: N_D \subset \text{term}(n) \wedge v_0 \not\subset \text{term}(n)\}$ 至少有 1 个极小元节点 n_2,n_2 是常规节点且符号为正.

我们需要证实 n_2 能否出现在攻击者串 p 上.

S:S 的迹为$\langle -gh,+g,+h\rangle$,不是一般性,$\text{term}(n_2)=g$ 和 $\text{term}(n_2)=h$ 的情况是对称的. 集合 $U=\{m \in C: m \prec n_2 \wedge gh \subset \text{term}(m)\}$ 有极小元节点 m_1,因为 $\text{term}(\langle p,1\rangle)=-gh$ 且$\langle p,1\rangle \in U$.

S:如果 $gh \subset \text{term}(m_1)$,$m_1$ 是 S 型攻击者串 p'上的 1 个正节点,那么 $gh \subset \text{term}(\langle p',1\rangle)$. $\langle p',1\rangle \prec m_1$,与 m_1 是 U 上的极小元矛盾.

E. (D.):如果 $gh \subset \text{term}(m_1)$,$m_1$ 是 E(或 D)型攻击者串 p'上的 1 个正节点,那么 $gh \subset \text{term}(\langle p',2\rangle)$. $\langle p',2\rangle \prec m_1$,与 m_1 是 U 上的极小元矛盾.

C:如果 $gh \subset \text{term}(m_1)$,$m_1$ 是 E(或 D)型攻击者串 p'上的 1 个正节点且 m_1 是 U 上的极小元,那么 $\langle p',3\rangle = m_1$,$\text{term}(\langle p',1\rangle)=\text{term}(n_2)$且 $\text{term}(\langle p',1\rangle) \prec n_2$,与 n_2 是 S 上的极小元矛盾.

引理 3 在 t 中,存在 1 个节点 n_1 在 n_2 之前,使得 $H(f_k(TID)) \oplus f_{k'}(TID) \subset \text{term}(n_1)$.

从引理 1 和定义,我们知道 N_D 起源于 n_0,且唯一起源于 Σ. 由于 $v_0 \subset \text{term}(n_0)$且 $v_0 \not\subset \text{term}(n_0)$,所以 $n_2 \neq n_0$. 因此,N_D 不源于 n_2 且在之前必有 1 节点 n_1 使得 $v_0 \subset \text{term}(n_1)$,由 n_2 的极小性,$H(f_k(TID)) \oplus f_{k'}(TID) \subset \text{term}(n_1)$.

引理 4 包含 n_1 和 n_2 的正规串 t 在 C 上,且是 1 个响应者串.

如果 t 是 1 个发起者串,紧跟着 n_1 的应该是 1 个负节点. 但 n_2 是 1 个正节点,所以 t 是 1 个响应者串. t 的最后 1 个节点 n_2 也包含在 C 中.

定理 3 和 4 证明了命题 1.

2.3.2 *秘密属性的证明*

命题 2 假设(1)Σ 是 P_{OT}串空间,C 是包含发起者串 $s \in \text{Init}[\text{DB},\text{Tag},N_D,N_T]$的簇;

(2)$k \notin K_P$;

(3)$N_D \neq N_T$,N_D 唯一起源于 Σ;则对所有节点 $m \in C$,当 $N_D \subset \text{term}(m)$时,必有 $H(f_k(TID)) \oplus f_{k'}(TID) \subset \text{term}(m)$或者 $H(f_{k'}(TID) \parallel N_D \parallel N_T) \subset \text{term}(m)$.

证明 设 $H(f_k(TID)) \oplus f_{k'}(TID)=v_0$,$H(f_{k'}(TID) \parallel N_D \parallel N_T)=v_1$

考虑集合 $F=\{n \in C: N_D \subset \text{term}(n) \wedge v_0 \not\subset \text{term}(n) \wedge v_1 \not\subset \text{term}(n)\}$.

设 F 非空,则 F 至少有 1 个极小元. 下面先证明这些极小元不是常规节点,再证明它们不是攻击节点,因此 F 为空,命题得证.

设 m 是 F 的极小元,且是常规节点,则 m 的符号为正. 在 s 中只有 n_0 的符号为正,但 $v_0 \subset \text{term}(n_0)$,所以 m 不在 s 上. 又 N_D 唯一产生于 n_0,所以 m 不在其他常规 strand $s' \neq s$ 上,故 m 不可能是常规节点.

F 的极小元不是攻击节点的证明与引理 1 极为相似. 由于 $S=\{n \in C: N_D \subset \text{term}(n) \wedge v_0 \not\subset \text{term}(n)\}$ 的极小元不是攻击节点上,那么 F 的极小元也一定不是攻击节点上.

综上所述,F 只能为空,所以 N_D 只能以协议规定的加密形式出现,因此是保密的.

命题 3 假设

(1)Σ 是 P_{OT}串空间,C 是包含发起者串 $s \in \text{Init}[\text{DB},\text{Tag},N_D,N_T]$的簇;

(2)$k \notin K_P$;

(3)N_D 唯一起源于 Σ;那么 C 包含响应者串 $t \in \text{Resp}[\text{DB},\text{Tag},N_D,N_T]$的前两个节点.

集合$\{m \in C: H(f_{k'}(TID) \parallel N_D \parallel N_T) \subset \text{term}(m)\}$是非空的,因为它包含节点$\langle s,2\rangle$,故存在极小元节点 m_0. 现在,对于正规串 t,如果 m_0 在 t 上,那么 t 的迹为 $\text{Resp}[\text{DB},\text{Tag},N_D,N_T]$. 正规串 t 至少有两个节点在 C 上. 但是,如果 m_0 在攻击者串 t 上,那么 t 可能是 E 型攻击者,其迹为$\langle -N_T,-N_D,f_{k'}(TID),+H(f_{k'}(TID)$

$\| N_D \| N_T) \rangle$. 但是,它违背了定理 2,这意味着 N_D 不出现在节点$\langle t,2 \rangle$上. 协议中其他循环的证明在结构上类似,因此为了简便考虑就省去了.

3 结论

从本文中可以看到现今很多的 RFID 安全协议都存在各种漏洞,尤其是 RFID 的所有权转移的安全性更是需要我们去改善. 于是我们提出了一种新的 RFID 安全协议,它满足几种安全需求:前向和后向安全,抗重传攻击,防止信息泄露,相互身份验证和防 DoS 攻击. 而且该协议允许 RFID 系统中所有权的可转移性. 最后,该协议通过 BAN 逻辑和串空间证明其正确性和安全性.

[参考文献](References)

[1] Osaka K,Takagi T,Yamazaki K,et al. An efficient and secure RFID security method with ownership transfer[J]. Computational Intelligence and Security,2006,2:1 090-1 091.

[2] Thayer Fabrega F W,Herzog J C,Guttman J D. Strand space:providing security protocols correct[J]. J Compute Security,1999,7:191-230.

[3] Burrows M,Abadi M,Needham R. A logic of authentication[J]. ACM Transactions on Computer,1990,8(1):18-36.

[4] Yiqi G,Jie Z,Hwangkye C. An improved RFID Security method with ownership transfer[C]//Proceedings of ICTC. Seoul,Korea,2011:594-596.

[5] Chen H B,Lee W B,Zhao Y H,et al. Enhancement of the RFID security method with ownership transfer[C]//Proc Int Conf Ubiquitous Inform Manage. Communication,Suwan,Korea,2009:251-254.

[6] Lei H,Cao T. RFID protocol enabling ownership transfer to protect against traceability and DoS attacks[C]//Proc 1st Int Symp Data,Privacy E-Commerce. Chengdu,2007:508-510.

[7] Jappinen P,Hamalainen H. Enhanced RFID security method with ownership transfer[J]. International Conference on Computational Intelligence and Security,2008,2(13-17):382-385.

[8] Eunjun Y,Keeyoung Y. Two security problems of RFID security method with ownership transfer[C]//Proc IFIP Int Conf Netw. Parallel Compute,Shanghai,2008:68-73.

[9] Song B,Mitchell J. Scalable RFID security protocols supporting tag ownership transfer[J]. Computer Communications,2011,34(4):556-566.

[10] 张兵,马新新,秦志光. Hash 运算的 RFID 认证协议分析和改进[J]. 计算机应用研究,2011,28(11):4 311-4 314.
Zhang Bing,Ma Xinxin,Qin Zhiguang. Analysis and improvement of hash-based RFID authentication protocol[J]. Application Research of Computers,2011,28(11):4311-4314.(in Chinese)

[责任编辑:顾晓天]