

基于杂凑函数的 RFID 标签数据安全研究与实现

李秀芝, 霍 华, 马 林

(河南科技大学 电子信息工程学院, 河南 洛阳 471003)

摘 要: 提出一种改进的基于杂凑函数的 RFID 标签数据的安全认证算法. 该算法采用 RFID 标签和读写器的双向认证机制, 并利用 BAN 逻辑对其进行形式化分析, 结果表明该算法具有前行安全性、重传攻击、哄骗攻击、位置跟踪、不可分辨性等特点, 能够较好的解决 RFID 标签数据的安全隐患问题.

关键词: 射频识别; 杂凑函数; BAN 逻辑; 射频标签; 安全

中图分类号: TP39

文献标识码: A

文章编号: 1000-7180(2010)07-0185-05

The Research and Implementation of RFID Tag Data Security Based on Hash

LI Xiu-zhi, HUO Hua, MA Lin

(Electronic Information Engineering College, Henan University of Science and Technology, Luoyang 471003, China)

Abstract: Proposes an improved RFID tag data security authentication algorithm based on Hash. The algorithm uses two-way authentication mechanism of the RFID tag and reader, and by the BAN logic to formal analysis. The result show that the algorithm possess forward security, replay attack, spoofing attack, location tracking, distinguish ability and so on. So the algorithm can better solve the RFID tag and reader security issues.

Key words: RFID; Hash; BAN logic; RFID tag; security

1 引言

射频识别 (Radio Frequency Identification, RFID) 技术是 20 世纪 80 年代末发展起来的新型的 non-contact 自动识别技术^[1]. 随着射频识别的广泛应用, RFID 标签数据的安全问题也日益突出^[2]. 目前, RFID 标签数据存在的安全问题主要有: 不具有可靠的信息安全机制的射频标签数据可以被未授权的读写器读取; 携带 RFID 标签的用户可以被跟踪; RFID 标签中的数据可以被克隆, 甚至只要用重放攻击、哄骗攻击就可以伪装标签等. 这些问题成为 RFID 急待解决的问题及研究热点之一. 因而, 吸引了业界众多安全专家的关注和投入, 并已提出了各种解决方案和策略. 但目前已提出的方案和策略都

存在着某种弱点和漏洞.

文中提出一种改进的射频识别的安全算法, 它将杂凑函数和密钥加密算法相结合, 有效地解决 RFID 标签数据的机密性、真实性、完整性、不可否认性等安全问题, 并利用 BAN 逻辑对该安全算法进行形式化分析和推理证明.

2 RFID 安全解决方法

基于密码学的 RFID 安全解决方法能有效的加强 RFID 标签数据的安全性能、保护消费者隐私、防止信息泄露. 下文将介绍三种 RFID 安全解决方法, 并分析其优缺点.

2.1 摘要锁方法

摘要锁方法中 RFID 标签可以被“锁定”. 在锁

收稿日期: 2009-05-17; 修回日期: 2009-08-25

基金项目: 国家自然科学基金项目(60743008); 河南省科技攻关计划项目(072302110010); 河南省教育厅自然科学基金基础研究计划项目(2007520013)

定状态下,标签对 RFID 读写器发出的除解锁信号之外的所有询问信号都将返回解锁密码的摘要值 Meta-ID,而不是标签的 ID,此方法基于单向摘要函数^[3].

基于单向摘要函数的逆向运算困难,此方法可防止未授权用户利用 Meta-ID 计算 Key 值,从而达到防止标签 ID 泄露的目的.但摘要锁方法的一个缺点是无法抵抗“中间人攻击”,一个攻击者可以询问标签的 Meta-ID,然后以重放攻击方式将其发给合法读写器,读写器按照规定的流程将返回对应的 Key 值,攻击者便可以利用 Key 值得到标签的 ID.

2.2 重加密方法

重加密方法可重命名标签,使得攻击者无法跟踪和识别标签^[4].为了增强 RFID 系统的安全性,重加密方法使用目前流行的公钥加密机制.而公钥加密机制运算量大、资源需求较多,由于受成本的影响,RFID 标签的运算资源受到严格限制,所以重加密方法将密码运算交由外部代理完成,标签本身不执行运算,只存储相关数据.

重加密方法的安全性依赖于公钥加密机制和摘要函数,安全性较高,但没有有效解决用户隐私问题.此方法所需资源也比较多,虽然 RFID 标签无须执行密码运算,但加密代理设备、可视化机制验证设备等成本较大,另外,此机制还需要标签至少具备几百位的存储空间,这将增大标签的成本.因此重加密方法不适用于为普通低价值物品所设计的系统.

2.3 阻塞标签方法

阻塞标签方法是基于二进制树型查询算法,使用“阻塞标签”来达到保护 RFID 标数据安全的目的^[5].阻塞标签通过模拟标签 ID 的方式干扰算法的查询过程.阻塞标签可以模拟 RFID 标签 ID 的所有可能的集合,从而避免标签的 ID 被查询到.

阻塞标签方法的优点是 RFID 标签基本不需要修改,也不必执行密码运算,减少了投入成本,并且阻塞标签本身非常便宜,与普通标签价格相差不大,这使得阻塞标签方法可作为一种有效的保护 RFID 标签数据安全的工具.但同时阻塞标签方法也可能被用于进行恶意行为:通过模拟标签 ID,恶意阻塞标签能够超出规定保护 RFID 标签数据安全的范围,进而干扰正常的 RFID 标签数据的应用. RFID 读写器能够处理安全区域内的阻塞行为,但它的主要功能是查询此区域外的标签,因此恶意阻塞标签能对系统进行拒绝服务攻击,破坏 RFID 系统的正

常运行.

3 基于杂凑函数的 RFID 标签数据的安全算法研究

由于受标签本身成本所限,标签本身很难具备保证数据安全的能力.若没有可靠的安全机制,就无法有效的保护 RFID 标签中数据信息.这样,就面临了一个很大的安全问题.非法用户假冒合法用户利用读写器,直接与标签进行通信.这样,RFID 电子标签就很容易受到攻击,而对于读写式 RFID 电子标签,还将面临标签数据被篡改或删除的风险.因而一个完备的 RFID 安全方案必须能够保证电子标签中所包含的信息只能被授权的合法读写器访问.

3.1 标签和读写器的认证过程

在初始状态下,假定攻击者可以窃听到读写器和标签之间的无线通信,但读写器和后端数据库的通信是在一条用成熟的安全机制加以保证的有连接信道上进行的^[6].标签中存储标签的 ID 以及密钥 k ,且嵌入了一个杂凑函数(hash)运算^[7],且后端数据库存储所有合法标签的 ID 和密钥 k .读写器中含有一个随机数发生器.进行如下设定:

(1) $h_k(M)$:表示用密钥 k 对信息 M 进行单向杂凑函数运算,其中 M 是一个变长的敏感信息.标签出厂时已经存储 $R_0 = h_k(M)$;

(2) R_r :读写器产生的随机数;

(3) R_{t_i} :标签产生的第 i 个随机数;

(4) $\oplus$:异或运算符;

(5) $? =$:比较两者是否相等;

(6) $\rightarrow$:发送符.

基于杂凑函数的 RFID 安全算法如图 1 所示.

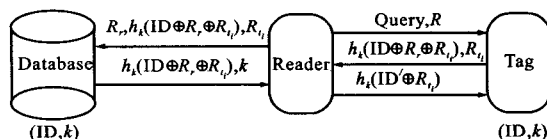


图 1 基于杂凑函数 RFID 安全算法

对图 1 的说明如下:

(1) 读写器发出询问指令 Query, 并将读写器产生的一个随机数 R_r 发送给电子标签.

(2) 标签计算 $R_{t_i} = h_k(\text{key} \oplus R_{t_{i-1}} \oplus R_r)$, 然后将随机数 R_r, R_{t_i} 以及自身的 ID 进行异或运算及基于共享密钥 k 的单行杂凑运算, 将得到的 $h_k(\text{ID} \oplus R_r \oplus R_{t_i})$ 连同随机数 R_{t_i} 一起发送给读写器.

(3) 读写器发送 R_r , 并转发 $h_k(\text{ID} \oplus R_r \oplus R_{t_i})$

和随机数 R_{t_i} 给后端的数据库系统;

(4) 后端数据库根据接收到的 R_{t_i} 、 R_r 及存储在数据库中的密钥 k , 查找是否存在一个 ID' , 使得 $h_k(ID' \oplus R_r \oplus R_{t_i}) = h_k(ID \oplus R_r \oplus R_{t_i})$. 如果存在, 则证明了标签的合法性. 后端数据库通过安全的通道将 $h_k(ID' \oplus R_r \oplus R_{t_i})$ 和 k 传送给读写器. 否则标签是非法标签.

(5) 读写器利用密钥 k 计算得到 $h_k(ID' \oplus R_{t_i})$ 并发送给标签.

(6) 标签验证 $h_k(ID' \oplus R_{t_i}) = h_k(ID \oplus R_{t_i})$. 如果相等, 则证明了读写器的合法性, 否则读写器是非法读写器.

这样系统就完成了 RFID 电子标签和读写器的相互认证过程, 上述过程保证了 RFID 标签数据的安全性.

3.2 安全性能分析

(1) 根据 hash 函数的定义和性质可知, hash 函数具有单向性, 即使攻击者破译了标签的当前输出, 攻击者无法根据当前获得的标签输出来回溯标签的历史数据, 因此该方案具有前行安全性.

(2) 由于 hash 函数具有抗碰撞性以及 R_{t_i} 的随机性, 即便攻击者执行如下操作: 读写器发送 Query, R_r 认证请求, 攻击者监听获得标签输出 $h_k(ID \oplus R_r \oplus R_{t_i})$ 和 R_{t_i} . 当读写器再次发送 Query, R_r 认证请求时, 攻击者将上次监听得到的数据发送给读写器, 达到伪装合法标签的目的. 但由于 $h_k(ID \oplus R_r \oplus R_{t_i})$ 的抗碰撞性和 R_{t_i} 的随机性, $h_k(ID \oplus R_r \oplus R_{t_i}) \neq h_k(ID \oplus R_r \oplus R_{t_j})$, $R_{t_i} \neq R_{t_j}$, 其中, $i \neq j$. 因此能够抵御重传攻击.

(3) 在 RFID 标签和读写器的无线通信中, 即便攻击者伪装成合法读写器发送 Query, R'_r 至标签, 标签响应请求, 输出 $h_k(ID \oplus R'_r \oplus R_{t_i})$ 、 R_{t_i} . 当合法读写器再次发出认证请求时, 攻击者发送刚才标签的响应以欺骗读写器. 但是由于每次认证读写器都会产生一个随机数 R_r , $h_k(ID \oplus R_r \oplus R_{t_i}) \neq h_k(ID \oplus R'_r \oplus R_{t_i})$, 也即攻击者不可能产生标签的正确响应, 因此可以防止哄骗攻击.

(4) 在标签和读写器的相互认证过程中, 标签对每次询问的反映是变化的, 即便攻击者伪装成合法读写器发送 Query, R'_r 至标签, 从而得到标签输出. 攻击者试图通过分析 $h_k(ID \oplus R'_r \oplus R_{t_i})$ 、 R_{t_i} 来确定是哪张标签的输出. 但是, hash 函数的抗碰撞性

和 R_{t_i} 的随机性阻止了攻击者对标签的通信量分析攻击, 因此攻击者无法根据特定的输出对标签实施位置跟踪.

(5) 由于 hash 函数的单向性以及使用了随机数, 即使攻击者获得了多张标签的输出, 也无法分辨出某一张标签的输出, 即 $h_k(ID' \oplus R_r \oplus R_{t_i}) \neq h_k(ID \oplus R_r \oplus R_{t_i})$; 即使获得了同一张标签的多次输出, 也无法分辨出该标签的某一次输出, 即 $h_k(ID \oplus R_r \oplus R_{t_i}) \neq h_k(ID \oplus R_r \oplus R_{t_j})$, 因此具有不可分辨性.

4 算法的安全性推导与分析

4.1 BAN 逻辑

BAN 逻辑是由美国 DEC 公司的研究人员 M. Burrows, M. Abadi 和 R. Needham 提出的一种可用于认证协议形式化分析的逻辑^[8], BAN 逻辑由一系列命题和逻辑规则组成. 采用 BAN 逻辑来分析通信协议的安全性, 揭示了一些非形式化方法很难发现的缺陷和冗余, 通过严格的数学推理, 能够很好地解决协议的认证性问题, BAN 逻辑已成为最有影响的认证协议形式化证明的有效方法. 因而文中选用 BAN 逻辑对 RFID 标签数据的安全协议的认证部分进行形式化分析和推理证明.

BAN 逻辑包含三种处理对象: 主体、密钥和公式. 其中公式也称作语句或命题, 可以是单独的主体或密钥. P 和 Q 表示主体变量, A 和 B 表示普通主体, K 表示共享秘密变量, X 和 Y 表示公式变量, S_i 和 R_r 表示临时值.

4.2 BAN 逻辑的基本表达式

$P \models X$: P 相信 X , 即 P 认为 X 为真.

$P \models \sim X$: P 曾经说过 X , 即主体 P 在某一时刻曾发送过包含 X 的信息.

$P \triangleleft X$: P 看到过 X , 即 P 曾收到包含 X 的信息.

$P \Rightarrow X$: P 对 X 有管辖权, 或者仲裁权.

$\#(X)$: X 是新鲜的, 即 X 没有使用过.

$P \stackrel{K}{\leftrightarrow} Q$: k 是 P 和 Q 的一个共享密钥, 且 K 是好的密钥.

$\{X\}_K$: 表示用 K 加密 X .

4.3 BAN 逻辑的主要推理规则

BAN 逻辑中共有 19 条推理规则, 下面仅列出本文使用的 7 条规则(横线上表示前提, 横线下表示结论).

(1) 消息意义规则 $\frac{P \models P \leftrightarrow^K Q, P \triangleleft \{X\}_K}{P \models Q \mid \sim X}$

(2) 随机数验证规则

$$\frac{P \models \#(X), P \models Q \mid \sim X}{P \models Q \models X}$$

(3) 管辖权规则

$$\frac{P \models Q \mid \Rightarrow X, P \models Q \models X}{P \models X}$$

(4) 新鲜规则 $\frac{P \models \#(X)}{P \models \#(X, Y)}$

(5) 信仰规则 $\frac{P \models X, P \models Y}{P \models (X, Y)}$

(6) 信仰规则 $\frac{P \models (X, Y)}{P \models X, P \models Y}$

(7) 良好密钥规则

$$\frac{P \models P \overset{\text{GoodKey}(k)}{\leftrightarrow} Q, P \triangleleft \{X\}_k}{P \models Q \models X}$$

4.4 BAN 逻辑形式化分析

在本算法中将电子标签视为主体 B , 读写器视为主体 A , 后端数据库系统视为主体 S . B 与 S 在初始化时已共享密钥 k , 将读写器与后端数据库系统之间的安全通信模型假设为 A 与 S 利用一个安全的良好密钥 K_{as} , 目的是验证 A 和 B 的合法性.

4.4.1 建立协议的初始假设集合

$$\begin{aligned} B \models B \overset{k}{\leftrightarrow} S; A \models A \overset{K_{as}}{\leftrightarrow} S; \\ A \models S \Rightarrow ID; B \models S \Rightarrow A \overset{K_{as}}{\leftrightarrow} S; \\ B \models \#(R_t); A \models \#(R_r); \\ S \models A \models \#(R_r); S \models A \overset{K_{as}}{\leftrightarrow} S; \\ S \models B \overset{k}{\leftrightarrow} S; S \models \text{Goodkey}(K_{as}); \\ A \models \text{Goodkey}(K_{as}) \end{aligned}$$

4.4.2 构建协议的理想化模型

$M_1 A \rightarrow B$: A 向 B 发送认证请求 $\{\text{query}, R_r\}$

$M_2 B \rightarrow A$: B 向 A 发送 $\{(ID, R_r, R_t)_k, R_t\}$

作为应答

$M_3 A \rightarrow S$: A 向 S 发送 $\{R_r, (ID, R_r, R_t)_k, R_t\}_{K_{as}}$

$M_4 S \rightarrow A$: S 向 A 发送 $\{(ID', R_t)_k, ID'\}_{K_{as}}$

$M_5 A \rightarrow B$: A 向 B 发送 $\{(ID', R_t)_k, A \overset{K_{as}}{\leftrightarrow} S\}_k$

在此基本模型中 $M_1 M_2 M_3 M_4 M_5$ 表示 5 条消息, 消息 M_4 中 ID' 说明了标签的合法性, 消息 M_5 中 $A \overset{K_{as}}{\leftrightarrow} S$ 说明了读写器的合法性.

上述协议的预期目标是: $A \models ID, B \models A \overset{K_{as}}{\leftrightarrow} S$. 也即是经过读写器和标签的相互验证后, 读写器和标签均能得知对方是合法的.

4.4.3 利用 BAN 逻辑进行推理证明

消息 M_1 省略, 因为它对分析协议的逻辑属性没有作用, 与分析论证无关.

(1) 由模型中的消息 M_2 , 可以得到 $B \triangleleft R_t$, $B \triangleleft (ID, R_r, R_t)_k$, A 不理解加密后内容, 但可以转发给 S .

(2) 消息 M_3 可知 $S \triangleleft \{R_r, (ID, R_r, R_t)_k, R_t\}_{K_{as}}$, 加上初始假设: $S \models B \overset{k}{\leftrightarrow} S$ 和 $S \models \text{Goodkey}(K_{as})$, 利用推理规则(7), 可以得到 $S \models \{R_r, (ID, R_r, R_t)_k, R_t\}$. 规则(6)可以得到 $S \models \#(R_t)$, $S \models \#((ID, R_r, R_t)_k)$. 由假设 $S \models B \overset{k}{\leftrightarrow} S$, 利用规则(1)可得 $S \models B \sim \{ID, R_r, R_t\}$. 由假设 $A \models \#(R_r)$, $S \models A \models \#(R_r)$ 及规则(4)可得 $A \models \#(ID, R_r, R_t)$, $S \models \#(ID, R_r, R_t)$, 得 $S \models \#(R_r)$, $S \models B \sim \{ID, R_r, R_t\}$, $S \models ID$. 于是 S 发送消息 M_4 .

(3) 由消息 M_4 可知 $A \triangleleft \{(ID', R_t)_k, ID'\}_{K_{as}}$, 且 $A \models A \overset{K_{as}}{\leftrightarrow} S$, $A \models \text{Goodkey}(K_{as})$, 利用规则(7)可推得 $A \models S \models ID'$, 加上初始假设 $A \models S \Rightarrow ID'$, 利用规则(3)得到 $A \models ID'$.

(4) 由消息 M_5 可知 $B \triangleleft \{(ID', R_t)_k, A \overset{K_{as}}{\leftrightarrow} S\}_k$, 加上初始假设 $B \models S \Rightarrow B \overset{k}{\leftrightarrow} S$, 根据规则(1)得到 $B \models S \sim \{(ID', R_t)_k, A \overset{K_{as}}{\leftrightarrow} S\}$, 由初始假设 $B \models \#(R_t)$ 及规则(4)得到 $B \models \#(ID', R_t)_k$, $A \overset{K_{as}}{\leftrightarrow} S$. 再利用规则(2)可得到 $B \models S \models \{(ID', R_t)_k, A \overset{K_{as}}{\leftrightarrow} S\}$, 利用规则(6) $B \models S \models A \overset{K_{as}}{\leftrightarrow} S$, 加上初始假设 $B \models S \Rightarrow A \overset{K_{as}}{\leftrightarrow} S$ 由规则(3)可得到 $B \models A \overset{K_{as}}{\leftrightarrow} S$.

通过 BAN 逻辑对文中提出的安全算法进行形式化分析, 可以推导出 $A \models ID'$ 和 $B \models A \overset{K_{as}}{\leftrightarrow} S$, BAN 逻辑的推理结果证明了该算法的安全性, 达到了读写器和标签合法身份认证的安全目标, 通过 BAN 逻辑的分析和推理证明实现了该安全算法的

预期目标,因此 RFID 标签数据的安全性得到了保障。

5 结束语

文中提出了一种基于杂凑函数的 RFID 标签数据安全的研究方案,在本方案中 RFID 标签仅需要一个 hash 函数电路,成本较低,比较适合目前的实际情况和成本控制目标。同时,在保持低成本的前提下对该方案抵抗各种类型的攻击进行了分析,并通过 BAN 逻辑对该方案中的认证功能部分进行了形式化分析。结果表明本方案能够对读写器和标签的合法身份进行有效的双向认证、能够有效的抵御重传攻击、哄骗攻击、位置跟踪等。通过与现有的安全协议技术比较具有保护全面、低成本、低的计算量、便于扩展、适合于分布式数据库环境,能够有效的解决当前 RFID 标签数据面临的安全问题,非常适合用于建立仅具有有限资源的低成本标签的 RFID 系统的安全机制。

参考文献:

- [1] 彭昭,刘威,马选斌,等. RFID 系统安全与隐私问题研究[J]. 微电子学与计算机,2007,24(8):129-131.
- [2] 肖珊,郎为民,胡东华. 射频识别(RFID)安全解决方案研究[J]. 微计算机信息,2008(14):210-211.
- [3] 王连强,吕述望,韩小西. RFID 系统中安全和隐私问题的研究[J]. 计算机应用研究,2006(6):16-18.
- [4] Li Zhanglin, Lu Guizhang, Xin Yunwei. Application of reencryption technology in RFID security[J]. Computer Engineering,2008(3):160-162.
- [5] Juels A, Rivest R, Szydlo M. The blocker tag selective blocking of RFID tags for consumer privacy[C]// The 8th ACM Conference on Computer and Communications Security. New York, ACM Press, 2007:103-111.
- [6] Lin Guibin, Wang Yonghua, Zhan Yiju. RFID secure protocol based on random sequence[J]. Computer Engineering,2008(20):151-153.
- [7] Yuan Shuguang, Dai Hongyue, Lai Shengli. Hash-based RFID authentication protocol[J]. Computer Engineering, 2008(12):141-143.
- [8] Michael Burrows, Martin Abadi, Roger M Needham. A logic of authentication[J]. ACM Transactions on Computer Systems,2005,8(1):18-36.

作者简介:

李秀芝 女,(1982-),硕士研究生.研究方向为智能信息处理。
霍华 男,(1968-),博士,硕士生导师,副教授.研究方向为智能信息处理、光纤通道技术、嵌入式系统等。
马林 男,(1984-),硕士研究生.研究方向为光纤通道技术。

(上接第184页)

4 结束语

文中实现了基于嵌入微 Linux 内核的开机认证系统,并且采用 USB KEY 的方式分离存储硬盘重要信息及密钥,在密钥等重要信息的存储方面采用了成熟且加密效果优良的 MD5 与 DES 算法,从而增大了破解难度,很大程度上保障了计算机系统的安全。

参考文献:

- [1] Kephart J O. Biologically inspired defenses against computer viruses[C]// Proc. Int'l. Conf. on AI (IJCAI-95). Morgan Kaufmann, San Francisco, 1995:985-996.
- [2] White S R, Kephart J O, Chess D M. Computer viruses: a global perspective[C]// Proc. Fifth Int'l Virus Bulletin Conf. Virus Bulletin Ltd. England, Abingdon, 1995:165-181.
- [3] 廖金祥. 硬盘引导替换技术及其应用[J]. 武汉冶金科技大学学报,1998,21(1):1998.
- [4] Love R. Linux 内核设计与实现[M]. 2版. 陈莉君,译. 北京:机械工业出版社,2006.
- [5] 胡向东. 应用密码学[M]. 北京:电子工业出版社,2006.
- [6] 赵炯. Linux 内核完全注释[M]. 北京:机械工业出版社,2004.

作者简介:

马富达 男,(1985-),硕士研究生.研究方向为网络信息安全。
蔡皖东 男,(1955-),教授,博士生导师.研究方向为网络信息安全。