可证明安全的 RFID 通信安全协议 *

蔡庆玲[1],詹宜巨[1],刘 洋[2]

(1. 中山大学工学院 广州 510275;2. 中山大学信息科学与技术学院 广州 510275)

摘 要 通过对 RFID 系统特殊安全问题的系统研究,从可证明安全论证的角度出发,本文提出了一种可证明安全的 RFID 通信安全协议——rPAP。在随机预言模型下,使用形式化描述方式,系统地建立了 RFID 通信安全模型,并在该模型下,形式化地论证了 rPAP 协议的安全性。该协议适用于一般的 RFID 系统。

关键词 RFID;可证明安全;随机预言模型;哈希函数

1 引言

随着射频识别(radio frequency identification,RFID)技术的广泛应用,RFID 系统的安全问题也日益突出,特别是安全与隐私保护问题已严重阻碍了 RFID 技术的进一步发展,成为 RFID 技术发展急待解决的关键问题之一,已吸引了业界众多信息安全学者的关注和投入,并已提出了众多的解决方案。近期提出解决方案如:IBM 公司的"夹子标签"技术、Noisy Tags 法[1]及 Distance Bounding 法[2]等新的解决方案。IBM 公司的"夹子标签"技术不适用于需要信息重复读取的物流领域等。Noisy Tags 法需要增加额外的标签,而且存在安全漏洞无法抵抗重放攻击等。Distance Bounding 法增加了标签的认证时间,难以快速响应海量标签的识别。Tsudik 提出了 YA-YRAP 协议[3],由于时间戳的使用,虽然有效地降低了复杂性,但致使标签极易遭受拒绝服务的攻击,而导致标签的长久失效。Molnar 等提出了基于散列树的认证方案[4],该方案的每个标签的计算量是标签数量的对数且为变量。此外,如果一个标签被攻陷,整个散列树中其他标签的匿名性也会遭到破坏[5]。参考文献[6]提出基于 Hash 函数和二次剩余假设的安全通信协议,协议具有较强的安全与隐私保护性,但服务器需要求解两个二次同余方程和多达 8 次的 Hash 运算。参考文献[7]提出了基于密钥阵列的认证协议,由于使用密钥阵列,因而需占用较多的存储空间及运算时间。参考文献[8]提出了 RFID 系统可扩展安全认证协议,由于每次认证 ID 值都会发生变化,易受 DoS 攻击,一旦攻击成功将会导致标签的长久失效。

基于上述原因,本文提出了一种可证明安全的 RFID 通信安全协议——rPAP (provably secure authentication protocol for RFID)。从形式化论证的角度出发,通过对 RFID 系统特殊安全问题的研究,基于随机预言模型[9,10],提出了 RFID 系统的通信模型、攻击模型及其通信安全协议安全目标模型的形式化描述,建立了 RFID 通信的安全模型,并在

* 广东省基金资助项目(No. 9151027501000076)

该模型下，证明了 rPAP 的安全性。证明显示了本文提出的 RFID 通信安全模型能够有效地解决 RFID 系统特殊的安全问题。此外，本文所建立的 RFID 通信安全协议的安全目标模型能够有效地指导 rPAP 协议各项参数的选择，建立适合不同安全等级要求的 RFID 通信安全协议。

2 rPAP 的生成

2.1 系统初始化

RFID 系统初始化见图 1，由服务器为每一个标签分配一个惟一的标识码 ID（也可由制造商完成），服务器将标识码 ID 以及物品（贴有该标签的物品）的相关信息同时存储于标签和后端数据库，分别用 ID_t 和 ID_i 表示；再为每一个标签生成一个密钥 K（也可由制造商完成）也同时存储于标签和后端数据库中，分别用 K_t 和 K_i 表示。其中 K_t、ID_t 和 K_i、ID_i 是系统建立时由服务器产生并通过安全信道分别存储在相应标签及后端数据库并秘密保存的，故 K_t、ID_t 和 K_i、ID_i 在本系统中都被认为是安全保密的。

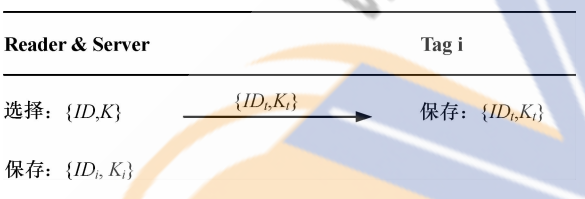

图 1 RFID 系统的初始化

- $Query$：读写器向标签发送的认证请求。
- ID_x：标签的标识码 ID，x 代表 t 或 i。
- R_r：读写器产生随机数。
- R_t：标签产生的随机数。
- $h_K(\ )$：带密钥 hash 函数，其中 K 为密钥。h: $\{0,1\}^* \rightarrow \{0,1\}^L$，其中 $\{0,1\}^*$ 表示长度为不确定的二进制串，$\{0,1\}^L$ 表示长度为 L 的二进制串。
- 0^μ 表示长度为 μ 的全“0”二进制串，1^μ：表示长度为 μ 的全“1”二进制串。
- ||为级联运算。
- ⊕为异或运算。
- →：发送。
- ==：比较两者是否相等。

2.2 认证过程

可证明安全的 RFID 通信安全协议如图 2 所示，认证步骤如下。

（1）Reader→Tag：读写器生成随机数 R_r，并向标签发送认证请求 $Query$，同时将 R_r 发送给标签。

（2）Tag→Reader→Server：标签接到读写器发来的认证请求（$Query$，R_r）后，也生成随机数 R_t，然后计算 $C_t=h_K(R_r||R_t||0^\mu)\oplus ID_t$。标签将 $\{C_t,R_t\}$ 发送给读写器，读写器再将 $\{C_t,R_t,R_r\}$ 转发给服务器。

（3）Server：服务器收到 $\{C_t,R_t,R_r\}$ 后，在后端数据库中寻找能使 $ID_i==C_i\oplus h_K(R_r||R_t||0^\mu)$ 成立的 ID_i 和 $K_i(1\leqslant i\leqslant n)$。如果 ID_i 和 K_i 存在，则认证通过，并转到第 4 步；否则，认证失败，停止操作。此次验证实现了读写器对标签的身份认证。

（4）Server→Reader→Tag：服务器计算 $C_i=h_K(R_r||R_t||1^\mu)\oplus ID_i$，并将 $\{C_i\}$ 发给读写器，读写器再将其转发给标签。

（5）Tag：标签收到 $\{C_i\}$，再验证 $ID_i==C_i\oplus h_K(R_t||R_r||1^\mu)$ 是否成立。如成立，则认证通过；否则，认证失败。此次验证实现了标签对读写器的身份认证。

由上述过程实现了标签和读写器的双向认证，此外对此认证过程再加上允许认证最大失败次数的限制。

3 RFID 通信安全模型

RFID 通信安全模型主要包括：RFID 系统模型；在 RFID 系统模型定义下，RFID 系统的攻击模型；RFID 通信安全协议的安全目标模型。在随机预言模型下[11,12]，针对 RFID 系统的特殊性安全要求建立 RFID 通信安全模型。

3.1 RFID 系统模型

RFID 系统是由多个主体（读写器、标签、后端服务器）和通信信道构成。对 RFID 通信安全协议进行安全性分析时，由于读写器和后端服务器之间的有线信道被认为是安

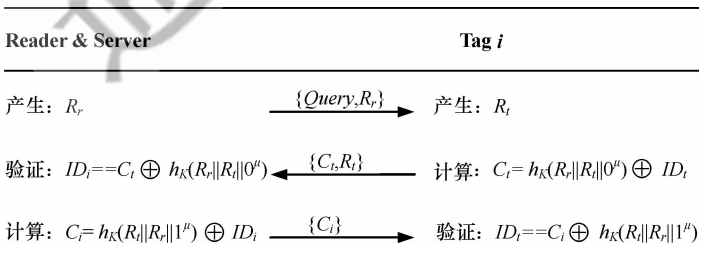

图 2 RFID 系统的认证过程

全信道，读写器和标签之间的无线信道是不安全信道，攻击者 A 所能获得的信息仅来自于无线信道。在建立 RFID 系统的可证明安全性形式化模型时，将读写器和后端服务器视为统一独立的实体，将读写器和后端服务器统称为读写器，此时，读写器既充当通信主体又充当认证主体。攻击者 A 可以控制所有读写器和标签的无线通信——符合 Doley-Yao 威胁模型。攻击者 A 可以任意地读取、插入、删除、篡改、延迟发送及重放任何消息，也可以在任何时候发起与任何实体的任意会话。

RFID 系统的实体有：阅读器集 I_R 和标签集 I_T。I_R 和 I_T 都是执行协议的参与者。攻击者 A 不属于这两个集合。形式上，rPAP 协议可表达为一个二元组 $P=(\Pi,\Phi)$。Π、Φ 都是安全参数 l^k 的多项式时间函数，$k\in N$。Π 定义了一个诚实阅读器 R 的行为；Φ 定义了一个诚实标签 T 的行为。

3.2 RFID 系统攻击模型

假设攻击者 A 是一个拥有 $Oracle\Pi^s_{R_i,T_j}$ 和 $\Phi^s_{T_j,R_i}$ 作为预言机(Oracle)的概率机器。攻击者 A 可以通过向 $Oracle\Pi^s_{R_i,T_j}$ 和 $\Phi^s_{T_j,R_i}$ 发送预定的质询，并从 Oracle 获得应答信息从而达到攻击的目的。协议运行期间，协议参与者和攻击者之间的交互仅通过 Oracle 质询来实现。这些 Oracle 质询刻画了攻击者 A 的实际攻击能力，攻击者 A 可以发送如下质询。

(1)$Execute(R_i, T_j, s, m_1, m_2)$：该质询刻画了对读写器、标签的被动攻击的实例 s。攻击者 A 通过监听协议参与者标签和读写器执行协议 P 的实例 s，可以获得协议 P 执行时标签和读写器之间交换的所有消息 m_1、m_2。

(2)$SendTag(T_j, s, m_1, m_2)$：该质询刻画了对标签的主动攻击的实例 s。攻击者 A 发送消息 m_1 给标签 T_j，并且接收到标签 T_j 的应答信息 m_2。

(3)$SendReader(R_i, s, m_1, m_2)$：该质询刻画了对读写器的主动攻击的实例 s。攻击者 A 发送消息 m_1 给读写器 R_i，并且接收到读写器 R_i 的应答信息 m_2。

(4)$Reveal(T_j)$：该质询刻画了标签私有存储空间内秘密信息 (ID_j,K_j) 的泄漏。

(5)$CorruptTag(T_j)$：该质询刻画了对标签的一种主动攻击，刻画了攻击者对标签的收买能力。使被收买后的标签 T_j 主动泄漏自己私有存储空间内的秘密信息 (ID_j,K_j)。

(6)$Test(T_j)$：该质询刻画了从 $Reveal(T_j)$ 获得标签的秘密信息 (ID_j,K_j)，用来度量一个 T_j 实例秘密信息 (ID_j,K_j) 的语义安全性。通过抛掷硬币 b，如果 $b=1$，返回标签存储的秘密信息 (ID_j,K_j)，如果 $b=0$，返回一个与标签秘密信息 (ID_j,K_j) 同等长度的随机数。

3.3 RFID 通信安全协议安全目标模型

对 RFID 通信安全需求进行分析。由于 RFID 系统安全问题的特殊性(保密性、流量分析、跟踪攻击、隐私泄漏等安全问题)，RFID 通信安全协议必须能够实现对明文信息的隐蔽，抵御对明文信息特性的统计，致使攻击者对所得信息及信息来源无法区分和识别，才能解决 RFID 系统特殊的安全问题。

在 RFID 系统中，攻击者最终攻击目的：获取 RFID 标签存储的秘密信息，为此，RFID 通信安全协议必须具有保密能力；对 RFID 标签 T_{j1} 和 T_{j2} 进行识别和区分，以便确认出它所攻击的目标，为此，RFID 通信安全协议必须确保 T_{j1} 和 T_{j2} 的不可识别和区分性。使用形式化描述上述对 RFID 通信安全协议功能的分析结果如下。

定义 1：识别成功事件 $Iden(A)$：对于任意一攻击者 A，攻击者 A 对某一 rPAP 协议的新鲜实例 P^s 执行一次 $Test(T_j)$ 质询，其结果为：$b'=b$。该事件定义为识别成功事件 $Iden(A)$。

定义 2：识别成功优势 $Adv_{rPAP,K}(A)$：令 $Q\subseteq\{E,S_T,S_R,R,C,T\}$，其中 E、S_T、S_R、R、C、T 分别表示 $Execute(R_i, T_j, s)$、$SendTag(T_j, s)$、$SendReader(R_i, s)$、$Reveal(T_j)$、$CorruptTag(T_j)$ 及 $Test(T_j)$ 几种 $Oracle$ 质询。攻击者的攻击目的是要识别和区分 T_{j1} 和 T_{j2}，以便确认出他所攻击的目标，在给定 rPAP 协议下，利用识别成功事件 $Iden(A)$，攻击者 A 对 T_{j1} 和 T_{j2} 的识别成功优势可定义为：$Adv_{rPAP,K}(A)=2Pr[Iden(A)]-1$。如果攻击者 A 的识别成功优势 $Adv_{rPAP,K}(A)$ 是可忽略的，则说协议 P 是 Q^* 安全的(其中 $j1$、$j2$ 可以相等)。

4 rPAP 安全性论证

4.1 安全证明

在上述建立的 RFID 通信安全模型下，对本文提出的 rPAP 协议的安全性进行论证。

定理 1 设攻击者的计算能力以多项式为界，基于带密钥哈希函数 $h_K(\ )$ 是安全的前提下，对 rPAP 协议进行攻击。设攻击者 A 执行 $SendTag(T_j, s)$、$SendReader(R_i, s)$ 的次数不大于 β_{send}，执行 $Execute(R_i, T_j, s)$ 的次数不大于 β_{exe}，则有：

$$Adv_{rPAP,K}(A)\leqslant 2(2\beta_{send}+\beta_{exe})/L_1+(2\beta_{send}+\beta_{exe})/L_2 \quad (1)$$

其中 $L_1=2^{|K|+|ID|}$，$L_2=2^{|Rr|+|Rt|}$，$|K|$、$|ID|$、$|Rr|$ 和 $|Rt|$ 表示相应的长度，如果攻击者 A 的识别成功优势 $Adv_{rPAP,K}(A)$ 是可忽略的，则说 rPAP 协议是安全的。

实验中,通过以实际攻击实验开始,推导出相关识别成功优势的概率公式,以证明攻击者没有攻击成功的优势。攻击者可以通过执行{E,S_T,S_R,R,C,T}几种 Oracle 质询,执行一系列的攻击,分别与 T_{j1} 和 T_{j2} 进行会话交互,获得会话集 $\Omega^A_p(T_{j1}, R_i)$和 $\Omega^A_p(T_{j2}, R_i)$。在每一个实验中,攻击者通过执行 $Test(T_j)$质询,获得每个识别成功事件 $Iden(A)$(正确地猜测($b'=b$)时)的概率 V_i,则攻击者识别成功优势:

$Adv_{rPAP,K}(A)=2Pr[Iden(A)]-1=\sum_{i=0}^{n-1}V_i$。

实验中,攻击者 A 在有限时间 τ 范围内,对 rPAP 协议进行攻击。攻击者 A 可以分别执行 β_{send} 次 $SendTag(T_j, s)$和 $SendReader(R_i, s)$质询,执行 β_{exe} 次 $Execute(R_i, T_j, s)$质询。我们模拟随机预言机 Oracles,并用结果维持哈希表队列:$\prod_{i=0}^{n-1}[a,h_K^i(a)]$,所有的{$E,S_T,S_R,R,C$} Oracle 质询都按 rPAP 协议真实地执行。

Epx1:在此实验中,攻击者的攻击目的是要获得 T_j 私有存储空间内的秘密信息(ID_j,K_j),可以通过执行{E,S_T,S_R,R,C}Oracle 质询,最终执行 $Test(T_j)$质询,可得攻击者成功获取 T_j 私有存储空间秘密信息的概率优势为:

$$V_0\leq(2\beta_{send}+\beta_{exe})/L_1, L_1=2^{|K|+|ID|} \quad (2)$$

Epx2:在此实验中,攻击者的攻击目的是要识别和区分 T_{j1} 和 T_{j2},以便确认出他所攻击的目标,攻击者可以通过执行{E,S_T,S_R,R,C,T} Oracle 质询,分别与 T_{j1} 和 T_{j2} 进行会话交互,最终执行 $Test(T_j)$质询,识别成功的概率优势分别如下。

(1)当 $j1\neq j2$ 时,则 T_{j1} 和 T_{j2} 是不同的标签,可得攻击者成功地识别不同标签的概率优势为:

$$V_1\leq(2\beta_{send}+\beta_{exe})/L_1, L_1=2^{|K|+|ID|} \quad (3)$$

(2)当 $j1=j2$ 时,则 T_{j1} 和 T_{j2} 是相同的标签,可得攻击者成功地识别不同标签的概率优势为:

$$V_2\leq(2\beta_{send}+\beta_{exe})/L_2, L_2=2^{|R_T|+|R_R|} \quad (4)$$

4.2 安全讨论

由上述 Epx1、Epx2 所得:$Adv_{rPAP,K}(A)=\sum_{i=0}^{n-1}V_i=2(2\beta_{send}+\beta_{exe})/L_1+(2\beta_{send}+\beta_{exe})/L_2$,可知,当 K、ID、R_r 和 R_t 4 个参数分别选择为 32 bit、64 bit、32 bit 及 32 bit 时,识别成功优势 $Adv_{rPAP,K}(A)$极小忽略不计,故 rPAP 协议是安全性。

此外,由上述分析可知,通过提高 K、ID、R_r 和 R_t 4 个参数的规格,可以有效地提高 rPAP 协议的安全性能,满足 RFID 标签更高的安全要求。

5 结束语

本文提出一种可证明安全的 RFID 通信安全协议——rPAP。从形式化论证的角度出发,建立了 RFID 通信的安全模型;并利用随机预言模型,进行了推理论证;通过证明攻击者的识别成功优势 $Adv_{rPAP,K}(A)$ 极小忽略不计,证明了 rPAP 协议的安全性。本文所建立的 RFID 通信安全协议的安全目标模型能够有效地指导 rPAP 协议各项参数的选择,建立适合不同安全等级要求的 RFID 通信安全协议。

参考文献

1 Claude C, Gildas A. Noisy tags: a pretty good key exchange protocol for RFID tags (NTP). In: Proceedings of CARDIS 2006, LNCS 3928, 2006

2 Chong H K, Gildas A. RFID distance bounding protocol with mixed challenges to prevent relay attacks. In: Proceedings of the 8th International Conference on Cryptology and Network Security, 2009

3 Tsudik G. YA-TRAP: yet another trivial RFID authentication protocol. In: Proceedings of the 4th Annual IEEE International Conference on Pervasive Computing and Communications Workshops, Washington, 2006

4 Molnar D, Soppera A, Wagner D. A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags. In: Proc Workshop on Selected Areas in Cryptography, 2006

5 Letri V, Burmester M, Medeirosde B. Universally composable and forward secure RFID authentication and authenticated key exchange. In: Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security, New York, 2007

6 Chen Y, Chou J, Sun M. A novel mutual authentication sheme based on quadratic residues for RFID system.Computer Networks, 2008, 52(12)

7 丁治国,郭立,王星洁.基于密钥阵列的 RFID 安全认证协议.电子与信息学报,2009,31(3):722~726

8 王云峰,焦保盈,李杰等. RFID 系统可扩展安全认证协议研究. 河北工业大学学报,2009,38(5):1~5

9 Kim H S, Choi J Y. The design and verification of RFID authentication protocol for ubiquitous computing. In:Proceedings of the 18th International Conference on Database and Expert Systems Applications, September 2007

10 冯登国. 可证明安全性理论与方法研究. 软件学报,2005,16(10)

11 Bellare M. Practice-oriented provable-security. In: Modern Cryptology in Theory and Practice, LNCS 1561, Berlin, Heidelberg: