一次性代理签名方案在移动代理技术中的应用研究^{*}

吴敏¹ 王汝传^{1,2}

(南京邮电学院计算机科学与技术系 南京210003)¹

(中国科学院研究生院信息安全国家重点实验室 北京100039)²

摘要 随着电子商务、网络管理等分布式计算应用的发展,移动代理技术日益受到重视。但移动代理本身存在的各种安全隐患,限制了移动代理技术的发展。鉴于此,本文在代理签名体制上提出了一种新型的可验证安全性的一次性代理签名方案,并通过将它结合到一个典型的移动代理电子商务应用实例中去阐述了该方案在移动代理系统中的应用,最后对其有效性和安全性进行了解析。

关键词 移动代理,代理签名,一次性签名方案

A Study on One-Time Proxy Signature Scheme and its Application in Mobile Agent Technology

WU Min¹ WANG Ru-Chuan^{1,2}

(Department of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003)¹

(State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, Beijing 100039)²

Abstract With the rapid increase of Distributed Computing Applications such as E-Business and Network Management, researchers have been attaching importance to Mobile Agent Technique. Aiming at a new concept of Multi-Mobile Agents' Cooperation, this paper proposes a new kind of security-proven one-time proxy signature scheme based on proxy signature mechanism for the serious security problems, and discusses its application in the mobile agent technology. Finally it makes the analysis for the security & validity of the scheme and its application.

Keywords Mobile agent, Proxy signature, One-time signature

1 引言

移动代理是20世纪90年代中期兴起的一种重要的分布式计算技术。它是一种独立的可执行程序,可以自主地在异构的网络上按照一定的规程移动,寻找合适的计算资源、信息资源,代表用户完成特定的任务。移动代理具有自主性、移动性、智能性、协作性等特点,在大型分布式系统问题上具有很强的适应性和优势,能有效降低网络通讯流量、减轻用户负担、提高交易效率。基于移动代理技术的各种应用范围十分广泛,覆盖电子商务^[2]、并行科学计算、分布信息检索和发布,即时监控及通报、个人助理等各方面。然而,基于移动代理的系统正面临着一些安全上的问题,如在代理执行任务过程中,涉及主机、代理、第三方相互之间的相互认证、通信与数据传输,于是容易引发一些相关的安全问题,如代理自身的数据、信息的可信度问题;主机或代理的数据被篡改或身份被冒充;交易抵赖行为,等等。本文在对代理签名体制的研究基础上提出了一种新型的可验证安全性的一次性代理签名方案,并将它应用到移动代理系统中去。研究表明该方案的应用既能增加 Internet 上各移动代理的可信度,又能保证其携带私密信息的安全性,同时能有效增强其交易活动的不可否认性。

本文第2节研究目前的代理签名方案和一次性数字签名方案,并提出一个具体的可结合这两种技术优势的移动代理电子商务应用案例。第3节通过该实例具体阐述了这种新型一次性代理签名方案在移动代理系统的应用。第4节讨论了该方案的性能和安全性。最后总结全文,并对下一步工作进行展望。

2 基于 RSA 的一次性代理签名方案

本节,主要讨论目前的代理签名方案和一次性数字签名方案,并提出一个具体的数字签名技术在移动代理电子商务中的应用实例。

2.1 系统参数

设 p, q 为大素数,且 $q | (p-1)$, $n = pq$, $1 < e < \phi(n) = (p-1)(q-1)$, 且 $\gcd(\phi(n), e) = 1$, $d \equiv e^{-1} \pmod{\phi(n)}$, $\text{hash}()$ 为抗冲突的哈希函数, O 为原始签名者,身份识别码为 ID_O , 拥有 RSA 密钥对 (n_o, e_o, d_o) , P 为代理签名者,身份识别码为 ID_P , 拥有 RSA 密钥对 (n_p, e_p, d_p) , V 为签名验证者, T 为可信的第三方,拥有 RSA 密钥对 (n_T, e_T, d_T) , S 为信任 T 的普通签名者。 req_o 为 O 的交易需求,如一项订购货物的需求表,包括所需货物的明细,价格底线,时间限制等, bid_p 为 P 的反馈信息。

2.2 代理签名方案

代理签名指当某签名人(本文称签名授权人)将签名权委派给其它人替自己行使签名权。在一个代理签名方案中,如果假设授权人 A 打算委托代理人 B 进行代理签名,则此签名方案应满足以下三个最基本条件:

可验证性:签名收方能够像验证 A 的签名那样验证 B 的签名;

可辨别性: A 的签名和 B 的签名应该完全不同,并且容易区分;

不可否认性: A 和 B 对签名事实不可抵赖,不可否认。

1996年, Mambo 等在文[1, 2]中第一次提出了代理签名

^{*} 本课题得到国家自然科学基金(60173037和70271050)、江苏省自然科学基金(BK2003105)、江苏省计算机信息处理技术重点实验室基金(kjs03061和kjs04)资助。吴敏 硕士研究生,主要研究方向是移动代理技术、分布式计算、计算机密码学和网格计算等。王汝传 教授,博士生导师,主要研究方向是计算机软件、计算机网络、信息安全、移动代理和虚拟现实技术等。

的概念,并根据代理授权的特点将代理签名分为三种,即完全代理(将授权人的私钥赋予签名者)、部分代理(产生一对新的密钥对)、带委任状的代理(发布一个关于代理授权信息的证书)。其中部分签名方案又可根据代理签名者是否受到保护细分为不保护签名者的和保护签名者的代理签名。由于代理签名方案在电子信息社会中具有重要意义,关于这方面的研究工作已经深入展开。

一般地,代理签名方案包括三个阶段,即:代理授权阶段,主要是要建立 O 和 P 之间的授权关系;代理签名阶段,指 P 代理 O 对消息签名;签名验收阶段主要是指任何第三方使用 O 、 P 的公钥检验代理签名是否合法。具体步骤如下:

1. 代理授权阶段

O 计算 $k = \text{hash}(ID_O, m_w)^{d_O} \bmod n_O$, 作为其对 (ID_O, m_w) 的 RSA 签名,并将 (ID_O, m_w, k) 通过安全通道传送给 P 。

2. 代理签名阶段

P 收到 (ID_O, m_w, k) 后首先要验证 $k^{e_O} \bmod n_O \stackrel{?}{=} \text{hash}(ID_O, m_w)$, 以确认受委托资料来源的可靠性。确认可靠以后, P 对消息 M, ID_O 和 m_w 进行 RSA 签名, 即计算 $x = \text{hash}(ID_O, m_w, M, ID_P)^{d_P} \bmod n_P$ 作为 P 对 (M, ID_O, m_w, ID_P) 的 RSA 签名, $y = \text{hash}(ID_O, m_w)^x \bmod n_O, z = k^x \bmod n_O$, 并公开 $(ID_O, m_w, ID_P, M, x, y, z)$ 。

3. 签名验收阶段

V 根据 $(ID_O, m_w, ID_P, M, x, y, z)$ 验证:

P 的签名: $x^{e_P} \bmod n_P \stackrel{?}{=} \text{hash}(ID_O, m_w, ID_P, M)$;

y 的有效性: $y \stackrel{?}{=} \text{hash}(ID_O, m_w)^x \bmod n_O$;

O 的签名: $z^{e_O} \bmod n_O \stackrel{?}{=} y$;

如果以上方程都验证正确, V 就可判定代理 P 关于消息 M 的签名为合法代理签名。

2.3 一次性签名方案

文[4]提出了一种基于 RSA 的 Fail-Stop 数字签名协议, 该方案用给定的密钥只对一则消息产生一次唯一的签名, 如果再次进行数字签名, 代理签名人的私密信息将被破解。该方案的优点是保证签名的唯一性, 以防签名权的滥用。

该协议包含四个阶段: 初始化阶段、密钥产生阶段、签名阶段和签名验证阶段。具体步骤如下:

1. 初始化阶段

T 选择随机数 $a \in Z_n^*$, 计算 $\beta = a^{e_T} \bmod n_T$ 。 T 公布 (a, n_T) , 并通过安全通道向 S 传送 (e_T, β) 。

2. 签名密钥产生阶段

S 接受 (e_T, β) 并选择四个不为 0 的整数 $k_1, k_2, k_3, k_4, k_i \in Z_n^*, 1 \leq i \leq 4$, 计算 $\beta_1 = a^{k_1} \beta^{k_3} \bmod n_T, \alpha_1 = a^{k_1} \beta^{k_1} \bmod n_T, \alpha_2 = a^{k_1} \beta^{k_2} \bmod n_T$, 并公布 $(\alpha_1, \alpha_2, \beta_1)$ 作为其签名公钥。

3. 签名生成阶段

对于任何消息 $x \in Z_n^*$, S 计算 $y_1 = k_1 x + k_2, y_2 = k_3 x + k_4$, 并公布 (y_1, y_2) 作为其对消息 x 的签名。

4. 签名验证阶段

V 根据 S 公布的 $(\alpha_1, \alpha_2, \beta_1)$ 和 (y_1, y_2) 验证方程 $\alpha_1^{y_1} \alpha_2^{y_2} \beta_1^{y_1} \stackrel{?}{=} \alpha_1^{e_T} \alpha_2 \bmod n_T$ 是否成立, 如果成立, 则认为 (y_1, y_2) 是 S 对消息 x 的正确签名。

在本方案中, 如果 S 企图用同样的密钥 (k_1, k_2, k_3, k_4) 对另外一则消息 x' 进行签名, 得到 (y_1, y_2) , 满足 $y_1' = k_1 x' + k_2, y_2' = k_3 x' + k_4$, 那么两次签名的结果将导致其密钥的泄露。因为从方程组

$$\begin{cases} y_1 = k_1 x + k_2, y_2 = k_3 x + k_4 \\ y_1' = k_1 x' + k_2, y_2' = k_3 x' + k_4 \end{cases}$$

可以立即计算出 (k_1, k_2, k_3, k_4) , 从而泄漏了 S 的私密信息, 所以 S 对一则消息用同样的密钥只能签名一次, 这种限制有效地控制 S 对签名权的滥用。

2.4 一次性代理签名方案

1. 代理授权阶段

O 随机选择四个不为 0 的整数 r_1, r_2, r_3, k_4 , 其中 $r_i \in Z_n^*, 1 \leq i \leq 4$, 计算

$k = \text{hash}(ID_O, m_w)^{d_O} \bmod n_O, s_i = r_i^{d_O} \bmod n_O$ 作为 O 对 (ID_O, m_w) 及 r_i 的 RSA 签名并将 $(ID_O, req_O, k, r_i, s_i)$ 通过安全通道传送给 P 。

2. 代理密钥产生阶段

P 收到 (ID_O, m_w, k) 后首先要验证 $k^{e_O} \bmod n_O \stackrel{?}{=} \text{hash}(ID_O, m_w), s_i^{e_O} \bmod n_O \stackrel{?}{=} r_i$ 以确认受委托资料来源和随机数的可靠性。确认可靠以后, P 计算 $k_i = d_P r_i \bmod n_P, 1 \leq i \leq 4, \beta_1 = \text{hash}(ID_O, m_w)^{k_1} k^{k_3} \bmod n_O, \alpha_1 = \text{hash}(ID_O, m_w)^{k_1} \beta_1^{k_1} \bmod n_O, \alpha_2 = \text{hash}(ID_O, m_w)^{k_2} \beta_1^{k_2} \bmod n_O$, 并公布 $(\alpha_1, \alpha_2, \beta_1)$ 作为其代理公钥。

3. P 代理 O 的一次性代理签名阶段

P 产生消息 M , 并对该消息进行一次代理签名。 P 计算 $y_1 = k_1 \text{hash}(ID_O, ID_P, m_w, M) + k_2, y_2 = k_3 \text{hash}(ID_O, ID_P, m_w, M) + k_4$, 并公布 (y_1, y_2) 作为其对消息 M 的签名并将 $(ID_O, ID_P, m_w, M, y_1, y_2)$ 。

4. 签名验收阶段

V 根据 $(ID_O, m_w, ID_P, M, r_i, y_1, y_2)$, 其中 $1 \leq i \leq 4$, 验证:

P 的代理签名钥的正确性: $\beta_1^{e_P \bmod n_P} \stackrel{?}{=} \text{hash}(ID_O, m_w)^{e_P \bmod n_P} k^{e_P \bmod n_P} \bmod n_O, \alpha_1^{e_P \bmod n_P} \stackrel{?}{=} \text{hash}(ID_O, m_w)^{e_P \bmod n_P} \beta_1^{e_P \bmod n_P} \bmod n_O, \alpha_2^{e_P \bmod n_P} \stackrel{?}{=} \text{hash}(ID_O, m_w)^{e_P \bmod n_P} \beta_1^{e_P \bmod n_P} \bmod n_O$;

P 的代理签名的有效性: $\text{hash}(ID_O, m_w)^{y_2} \beta_1^{y_1} \stackrel{?}{=} \alpha_1^{\text{hash}(ID_O, ID_P, m_w, M)} \alpha_2 \bmod n_O$ 。

如果以上方程都验证正确, V 就可判定代理 P 关于消息 M 的签名为合法一次性代理签名。

3 一次性代理签名方案在移动代理系统中的应用实例分析

本节具体分析了一个新型的代理一次性签名方案移动代理电子商务应用实例。假定源主机 O 欲在某网域内的若干执行主机上寻求一次最优航空票价, 寻求完毕之后再与拥有最优票价的目标主机签订预定票协议, 产生源主机的数字签名。源主机 O 创建移动代理 MA , 同时将数据信息 req (包括要求的航线地点、时间、可承受的最高价位等)、相关函数 (如可在票务中心进行航线的查询和利用查询结果对代理数据信息的更新, 如目前发现的最优航班名称, 价格等) 加载至该代理 (源主机还应采取相关的安全策略 (SSL 协议、加密封文等) 对传输中的主代理及所携机密数据进行保护, 见文 [10, 11], 但这不属于本文所讨论的内容, 故不赘述, 亦不分析其安全性和有效性)。移动代理在网络中漫游, 访问各票务中心, 执行相应的查询和更新任务, 当发现某中心提供的航班信息 bid 最优时, MA 便将该执行主机作为其预定航空票的目标主机, 并代表原主机对 req 和 bid 进行数字签名。在这样的场景下, 移动代理必须携带其原主机的私钥, 同时为了防止目标主机日后对其 bid 的抵赖, 还必须在数字签名中嵌入该目标主机的私钥。但这会导致该移动代理携带的原主机私钥暴露在目标执行主机上, 这是相当严峻的问题, 必须得到解决, 但目前尚没有出现最有效的研究方案。

本文提出的将代理签名方案和一次性数字签名方案结合起来的新型一次性代理签名方案可应用到该移动代理电子商务实例中去,能有效解决此类代理携带用户敏感数据信息的保护问题。在我们的方案中,移动代理将携带原主机的相关信息(req, ID 和原主机对 (req, ID) 的数字签名)在网络中漫游,当其完成最优航线的查询、最终确定欲定票的目的主机并欲进行订票行为时,目标主机将在检查该代理身份和其携带数据的真实性和有效性后代理原主机执行一次性代理签名,并将签名信息发回原主机,原主机可以据此验证此次移动代理执行任务的有效性。研究发现,该方案不仅可以保护原主机的私密信息,而且确保了原主机和目的主机对此次交易活动的不可抵赖性,和目的主机签名的一次有效性。

具体协议分析:

1. 原主机 O 准备移动代理阶段

O 随机选择四个不为0的整数 r_1, r_2, r_3, k_i , 其中 $r_i \in Z_n^*$, $1 \leq i \leq 4$, 计算 $k = \text{hash}(ID_O, req_0)^{d_0} \bmod n_0, s_i = r_i^{d_0} \bmod n_0$ 作为 O 对 (ID_O, req_0) 及 r_i 的 RSA 签名并将 $(ID_O, req_0, k, r_i, s_i)$ 和相应函数($Search()$ 和 $Update()$ 函数)加载到移动代理中去,并派遣其漫游到因特网上。注意:因为原主机并不知道具体的订票目的主机,所以无法指定确定的代理签名者。

2. 移动代理漫游、执行任务阶段

在本阶段中,移动代理访问各票务中心,执行相应的查询和更新任务,确定最优航班信息 bid , 锁定该主机作为其预定航空票的目标主机。

3. 目标主机 P 代理原主机签名阶段

1) P 对 MA 的验证

目标主机 P 将首先验证移动代理身份和任务的有效性。 P 验证方程 $k^{e_0} \bmod n_0 \stackrel{?}{=} \text{hash}(ID_O, req_0)$, 如果验证通过,则证明该代理确实由原主机 O 发出。

2) P 代理 O 签名密钥的产生

P 计算 $k_i = d_p r_i \bmod n_p, 1 \leq i \leq 4, \beta_1 = \text{hash}(ID_O, req_0)^{k_1} k^{k_1} \bmod n_o, \alpha_1 = \text{hash}(ID_O, req_0)^{\beta_1} \beta_1^{\beta_1} \bmod n_o, \alpha_2 = \text{hash}(ID_O, req_0)^{\beta_1} \beta_1^{\beta_2} \bmod n_o$, 并公布 $(\alpha_1, \alpha_2, \beta_1)$ 作为其公钥。

3) P 代理 O 的一次性代理签名阶段

P 产生消息 $msg = \text{hash}(ID_O, ID_P, req_0, bid_P)$, 并对该消息进行一次代理签名。 P 计算 $y_1 = k_1 \text{hash}(ID_O, ID_P, req_0, bid_P) + k_2, y_2 = k_3 \text{hash}(ID_O, ID_P, req_0, bid_P) + k_4$, 并公布 (y_1, y_2) 作为其对消息 msg 的签名并将 $(ID_O, ID_P, req_0, bid_P, y_1, y_2)$ 加载至移动代理后派遣其回到原主机 O 。

4. $O(V)$ 验证此次交易活动的有效性

O 验证 bid_P 是否符合 req_0 , 方程 $\beta_1^{e_p \bmod n_p} = \text{hash}(ID_O, req_0)^{k_1} k^{k_1} \bmod n_o, \alpha_1 = \text{hash}(ID_O, req_0)^{\beta_1} \beta_1^{\beta_1} \bmod n_o, \alpha_2 = \text{hash}(ID_O, req_0)^{\beta_1} \beta_1^{\beta_2} \bmod n_o, \text{hash}(ID_O, req_0)^{y_2} \beta_1^{\beta_1} \stackrel{?}{=} \alpha_1^{\text{hash}(ID_O, ID_P, req_0, bid_P)} \alpha_2 \bmod n_o$ 是否成立,如果二者都验证通过,则认为 $(\alpha_1, \alpha_2, \beta_1)$ 是 P 对本次交易的正确代理签名,而 (y_1, y_2) 是 P 对消息 msg 的正确代理签名,本次交易活动执行成功。

4 安全性分析

可以验证,该方案不仅可以保护原主机的私密信息,而且确保了原主机和目的主机对此次交易活动的不可抵赖性,和目的主机签名的一次有效性,是完全满足代理签名和一次性数字签名的各项要求。

(1) 移动代理携带信息的确认性

k 和 $s_i, 1 \leq i \leq 4$ 只能由 O 产生,因为 k 和 s_i 相当于 O 对

(ID_O, req_0) 及随机数 r_i 用私钥 d_0 的 RSA 数字签名,任何不知道 O 私钥的第三方都无法产生 k 和 s_i , 而任何知道 O 公钥 e_0 的第三方都可以验证其有效性。该 RSA 签名的安全性等同于 RSA 的安全强度。

(2) P 的代理密钥 k_1, k_2, k_3, k_4 的不可伪造性

代理密钥 k_i , 只能由接受到相应移动代理的主机 P 代理产生,任何不知道 P 私钥的其它主机都无法伪造。

(3) P 只能用该密钥对消息产生一次性有效签名

由于移动代理每次从事的商务任务的不尽相同,因此其每次携带的 req_0 具有信息的唯一性,同时因为 r_i 具有随机性,代理签名的主机每次产生的代理秘密密钥 $k_i (1 \leq i \leq 4)$ 也都是唯一的。另外,正如第3节对基于 RSA 的一次性签名协议的安全性分析,任何 P 如果企图用代理密钥 $k_i (1 \leq i \leq 4)$ 对其它消息进行伪造的代理签名,将会招致其代理密钥甚至其私钥的暴露,这对于 P 来说,是不可行的,综上, P 对每笔商务交易只能代理移动代理的主人作一次性代理签名。

(4) P 和 O 对本次交易活动的不可抵赖性

MA 携带的信息中包含了 O 的数字签名,而在执行任务完毕返回原主机 O 时,携带了 P 代理签名公钥和对此次交易的一次性代理签名,这使得 MA 的本次执行行动具有不可抵赖性,从而有效防止了 O 和 P 的事后抵赖引发的纠纷。

结束语 本文在研究基于 RSA 的代理签名和 one-time Fail-Stop 的基础上提出了可结合二者优势的新型一次性代理签名方案,将之应用到一个简单的移动代理电子商务实例中去,并讨论了其安全性问题。研究表明该方案的应用无论是在有效性还是安全性上都有着诸多优势,如可以有效解决对移动代理携带用户私密信息的保护等问题,当然由于技术的局限仍存在一些缺点。下一步工作的重点将放在对缺点的改进以及开发一个基于 Grasshopper 2.2(IKV++) 的具体应用该方案的完整移动代理商务交易平台。

参考文献

- Mambo M, Usuda K, Okamoto E. Proxy signature: Delegation of the power to sign messages. IEICE Trans. Fundamentals, E79-A: 9, 1996. 1338~1353
- Lee B, Kim H, Kim K. Secure Mobile Agent using Strong Non-designated Proxy Signature. Lecture Notes in Computer Science, 2001
- Kim H, Baek J, Lee B, Kim K. Secret Computation with Secrets for Mobile Agent using One-time Proxy Signature. In: Proc. of SCIS2001, 2001, 13: 845~850
- van Heyst E, Pedersen T. How to Make Efficient Fail-Stop Signatures. In Advances in Eurocrypt'92, LNCS 658, Springer Verlag, 1993. 366~377
- Susilo W, Safavi-Naini R, Pieprzyk J. RSA-Based Fail-Stop Signature Schemes. In: 1999 Intl. Workshops on Parallel Processing, Sep. 1999
- Lee B, Kim H, Kim K. Strong Proxy Signatures and Their Applications. In: Proc. of SCIS2001, Oiso, Japan, Jan. 2001
- Roth V. Mutual Protection of Cooperating Agents. In Jan Vitek and Christian Jensen, eds. Secure Internet Programming: Security Issues for Mobile and Distributed Objects, vol. 1603 of Lecture Notes in Computer Science, pp275~285
- Kim S, Park S, Won D. Proxy Signatures, Revisited. In: Y. Han et al, eds. Proc. of ICICS'97, LNCS 1334, Springer Verlag, 1997. 223~232
- Lee B, Kim H, Kim K. Strong Proxy Signature and its Applications. In: Proc. of SCIS2001, 2001. 603~608
- 王汝传, 徐小龙. 移动代理安全机制的研究. 计算机学报, 2002, 25(12): 1294Z~1301
- 王汝传, 赵新宁. 基于网络的移动代理系统安全模型研究和分析. 计算机学报, 2002, 26(4): 477~483
- 祁明, 许柏桐. 代理签名技术的研究和发展. 计算机应用研究, 2001, 18(9)