文章编号:1001 - 9081(2006)09 - 2109 - 02

一个安全的移动代理数据保护方案

柳 毅[1,2],张 凌[1]
(1. 华南理工大学 广东省计算机网络重点实验室,广州 510640;
2. 中山大学 广东省信息安全技术重点实验室,广州 510275)
(liuyi_xd@126.com)

摘 要:移动代理数据安全是移动代理系统面临的主要安全问题之一。基于 ElGamal 公钥体制,提出了一个安全的移动代理数据保护方案。对其分析的结果表明,该协议不仅满足所有的安全要求,而且可以使得同一移动代理多次经过同一主机,弥补了当前方案的不足。

关键词:移动代理; 数据安全; ElGamal 体制
中图分类号: TP393.08 **文献标识码**:A

A secure method of mobile agent data protection

LIU Yi[1,2], ZHANG Ling[1]
(1. *Guangdong Key Laboratory of Computer Network, South China University of Technology, Guangzhou Guangdong* 510640, *China*;
2. *Guangdong Province Key Laboratory of Information Security, Sun Yat-sen University, Guangzhou Guangdong* 510275, *China*)

Abstract: Data protection is one of security issues mobile agents have to face. In this paper, based on ElGamal scheme, a secure method for protecting mobile agent data was presented. Its security was analyzed. The results show that this method not only satisfies all security requirements but also makes the same mobile agent can visit the same host many times, which overcomes the shortcoming of the current protocols.

Key words: mobile agent; data protection; ElGamal scheme

0 引言

移动代理是通过在路由主机上运行自身所携带的指定代码来代替用户和路由主机之间进行交互,并且将交互的最终数据结果传回给用户,从而达到为用户服务的目的。因此,如何保护好移动代理的数据安全也就自然而然的成为研究移动代理系统安全的重要课题之一[1]。

对此,有一些相关方法被提了出来。Yee 曾利用局部认证来保护移动代理的数据[2],不过该方案存在不少安全隐患,如数据的前向完整性。Karjoth 等改进了 Yee 的结果,但是他们提出的方案[3]不能满足抗截断攻击。

在 Karjoth 方案的基础上,文献[4,5]分别给出了能够满足抗截断攻击的方案。但是,这两个方案都会泄漏不相邻主机的身份,而且要求同一个移动代理只能经过同一主机一次。即认定同一移动代理多次经过同一主机的行为为恶意行为。如果去掉这个要求,则这些方案不能满足安全性质。然而要实现该要求,一方面,移动代理对自己所经过的主机要做到"心中有数",以免再次经过;另一方面为了达到主机身份的保密性,又要提防将所经过的主机身份泄漏给其他主机。可见,该要求在实际中实现起来本身就比较困难,同时也为移动代理执行用户任务带来很大的不便。比如在购买商品时,移动代理很可能在比较多个商家提供的信息后,根据具体的价格和商家产品,才会决定去哪家购买。这样,移动代理首次经过商家时,可能只是进行信息的收集和比较;而比较后的结果会使得移动代理再次经过某些商家去购买合适的商品或者代表用户签署协议,也就必然会出现移动代理需要多次经过同一商家的情况。所以,这个要求对于移动代理的实际应用会带来很大的局限性。

本文提出了一个移动代理数据保护方案。通过分析得出,方案不仅满足所有安全要求,而且使得同一移动代理可以多次经过同一路由主机,增强了方案应用的灵活性。

1 符号标记及安全要求

1.1 符号标记

MA:移动代理;
uid:移动代理的唯一标识;
H_0:移动代理主人,即用户;
H_i:移动代理经过的路由主机,$i = 1,2,\cdots$;
TTP:可信第三方;
o_i:移动代理和 H_i 的交互结果,即 H_i 向用户提供的 offer(包括用户和主机的身份,以及详细的商品描述、价格、送货方式等),$i = 1,2,\cdots$;
O_i:对 o_i 采取一定的加密签名技术后,H_i 发给移动代理的信息,$i = 1,2,\cdots$;
x_i:主机 H_i 的私钥,$i = 1,2,\cdots$;
y_i:主机 H_i 的公钥,$i = 1,2,\cdots$;
$E_i(.)$:采用主机 H_i 的公钥对信息进行加密;
$S_i(.)$:主机 H_i 利用自己私钥对信息进行签名;
$h(.)$:安全抗碰撞的杂凑函数;
$A \rightarrow B:m$:主体 A 向主体 B 传送消息 m。

1.2 安全要求

假设移动代理访问了 m 个主机后,将要经过主机 H_{m+1}。这里引用 Karjoth 等给出的保护移动代理数据安全所需满足的安全要求[3]:

数据保密性 只有 H_0 可以从 O_i 中获取正确的 o_i。

收稿日期:2006 - 03 - 10; **修订日期**:2006 - 06 - 06 **基金项目**:广东省信息安全技术重点实验室开放基金资助项目

作者简介:柳毅(1976 -),男,江苏人,博士,主要研究方向:网络信息安全、移动代理; 张凌(1962 -),男,江西人,教授,博士生导师,主要研究方向:网络信息安全、计算机系统结构.

不可否认性　当 H_0 得到 o_i 后，H_i 不能否认 o_i 是它所给出的。

身份保密性　对于 o_i 的主机身份 H_i，只有 H_0 和 *TTP* 可以从 O_i 中提取获得，其他主机不能得到。

前向完整性　任何 $O_j(j < m)$ 都不能被修改。

公开可证实的前向完整性　如果需要，通过检查某个链式关系，任何实体都能够证实 O_i 的合法性。

抗插入攻击　不能插入新的 $O'_j(j < m)$。

抗删除攻击　任何 $O_j(j < m)$ 都不能被删除。

抗截断攻击　截断攻击是指 H_{m+1} 和一些主机共谋，将移动代理所携带 $O_0, O_1, \cdots, O_m$ 从某 $i(0 < i < m)$ 处截断，删除 i 处后面所有的 $O_k(i \leqslant k \leqslant m$ 或 $i \leqslant k \leqslant m)$，重新产生新的信息来替代它们。保护移动代理数据安全方案要求能抵制这种攻击。

2　安全的移动代理数据保护方案

2.1　方案描述

这里采用 ElGamal 公钥体制，公开的系统参数为：p, q, g。其中 p, q 是大素数，q 是 $p-1$ 的一个因子，g 是 z_p^* 中的一个 q 阶生成元。主机 H_i 的私钥为 $x_i < q$，公钥为 $y_i = g^{x_i} \bmod p$。

另外，为防止移动代理长时间在网络中徘徊，合乎实际的假设同一代理经过同一主机最多 $m(m > 1)$ 次。

（1）准备阶段

每个路由主机 $H_i(i = 1, 2, \cdots)$ 将其私钥 x_i 分拆为 $x_{i1}, \cdots, x_{im}$，要求满足 $x_{i1} + \cdots + x_{im} = x_i \bmod q$，并计算 $y_{i1} = g^{x_{i1}} \bmod p, \cdots, y_{im} = g^{x_{im}} \bmod p$，则必然有下式成立：

$$y_{i1} \times \cdots \times y_{im} = g^{x_{i1}} \times \cdots \times g^{x_{im}} = g^{x_{i1}+\cdots+x_{im}} = g^{x_i} = y_i \bmod p \quad (1)$$

（2）注册阶段

所有主机 $H_i(i = 1, 2, \cdots)$ 在可信第三方 *TTP* 处注册，发送如下信息：

$H_i \rightarrow TTP: E_{TTP}(S_i(H_i, y_{i1}, \cdots, y_{im}))$

TTP 解密 H_i 传来的信息，验证(1)式成立后，公开一个随机选择的消息 M_{TTP} 为下面的零知识证明使用（见执行阶段第1步）。

（3）执行阶段

移动代理 *MA* 从用户 H_0 发出时，携带一随机的 O_0。设 *MA*（唯一标识为 *uid*）经过主机 H_i，与 H_i 交互的结果为 o_i，H_i 进行如下步骤：

（a）计算 O_i

H_i 首先查看 *MA* 是第 $l(l \geqslant 1)$ 次经过自己，如果 $l < m$，计算 $O_i = E_{TTP}(H_{i-1}, H_i, H_{i+1}, R_{il}, S_i(x_{il}, uid), E_0(H_i, S_i(o_i))) \| h_i$，其中 R_{il} 为 H_i 产生的防止重放攻击的一次性随机数；如果 $l = m$，则 H_i 选择随机数 $k_i \in Z_q$，并计算 $r_i = g^{k_i} \bmod p$ 和 $s_i = x_{im} \cdot h(M_{TTP}, r_i) + k_i \bmod q$，然后计算

$$O_i = E_{TTP}(H_{i-1}, H_i, H_{i+1}, R_{im}, S_i(r_i, s_i, uid), E_0(H_i, S_i(o_i))) \| h_i$$

（b）计算所需的链式关系

$h_i = h(O_{i-1}, H_{i+1})$

（c）信息传递

$H_i \rightarrow H_{i+1}: \{O_k \mid 0 \leqslant k \leqslant i\}$

（4）验证阶段

当移动代理 *MA* 完成任务，它回到 *TTP*。*TTP* 首先逐个检查链式关系 h_i；然后解密每个 $O_i(i = 1, 2, \cdots)$ 得到相应的 $S_i(x_{il}, uid)$（*MA* 第 $l < m$ 次经过 H_i）或者 $S_i(r_i, s_i, uid)$（*MA* 第 m 次经过 H_i）。接着验证是否有 $y_{il} = g^{x_{il}} \bmod p$ 或者 $g^{s_i} = y_{im}^{h(M_{TTP}, r)} \cdot r \bmod p$（采用零知识证明是为了防止代理 m 次经过 H_i 后，会泄漏所有的 $x_{i1}, \cdots, x_{im}$，从而泄漏 H_i 的私钥 x_i）成立。

若以上检查均无异常，*TTP* 公开从该代理获得的所有 x_{il} 或 (r_i, s_i)。每个主机可以查看其中是否包含自己所提供的那部分信息，如果没有主机提出异议，*TTP* 最终将 *MA* 传回给用户 H_0。

2.2　方案安全性分析

数据保密性　只要所采用的加密算法是安全的，从 H_i 对信息的处理过程可以看出，只有 H_0 可以从 O_i 中获取正确的 o_i。

不可否认性　由于 O_i 中包含了 H_i 对 o_i 的签字，所以当 H_0 得到 o_i 后，H_i 不能否认 o_i 是由它所给出的。

身份保密性　只要加密系统是安全的，只有 *TTP* 解密 O_i 后获得提供 o_i 的主机身份 H_i，而用户 H_0 也可以从 o_i 提取相应的主机身份。虽然在协议验证阶段，*TTP* 公开了所有的 x_{il} 或 (r_i, s_i)，但是由于相应的 $y_{i1}, \cdots, y_{im}$ 并没有被公开，其他主机并不能通过 x_{il} 或 (r_i, s_i) 得知主机 H_i 参与了协议，依然符合身份保密性。

前向完整性　如果攻击者企图保持 O_m 完整，而修改 O_j，$j < m$。不妨假设 $j = m-1$，攻击者利用 O'_{m-1} 来替代 O_{m-1}。由于在 O_m 中包含链式关系 $h_m = h(O_{m-1}, H_{m+1})$，为了保持该关系，就要求有 $h(O_{m-1}, H_{m+1}) = h(O'_{m-1}, H_{m+1})$。因此，只要采用安全抗碰撞的杂凑函数 $h(.)$，攻击者就不能修改 O_{m-1}。归纳可得：攻击者不能修改任意 $O_j, j < m$。

公开可证实的前向完整性　通过检查链式关系 h_i，任何实体都能够证实 O_i 的合法性。

抗插入攻击　给定 $O_0, O_1, \cdots, O_m$ 后，链式关系保证了攻击者不能插入任何新的 $O'_j, j < m$。

抗删除攻击　链式关系也保证了任何 $O_j, j < m$ 都不能被删除。

抗截断攻击　由于在验证阶段，*TTP* 公开了所有的 x_{il} 或 (r_i, s_i)，每个主机都可以查看其中是否包含自己所提供的那部分信息。如果发生了截断攻击，假设某主机 H_j 发现自己所提供的 x_{jl} 或 (r_j, s_j) 不在其中，则 H_j 向 *TTP* 提供 H_{j-1} 传来的 $\{O_k \mid 0 \leqslant k \leqslant j-1\}$。*TTP* 在证实其中 H_{j-1} 的签名信息情况下，询问 H_{j-1}。这样一直追查下去，必定可以发现发动截断攻击的恶意主机。

3　结语

保护移动代理数据安全是移动代理技术是否能得到更广泛应用的关键安全问题之一。本文在指出了现有方案不足的基础上，基于 ElGamal 公钥体制，提出了一个安全的移动代理数据保护方案。分析结果表明，该协议满足所有的安全要求，而且可以使同一移动代理多次经过同一主机，弥补了当前方案的不足。

参考文献：

[1] BORSELIUS N. Mobile agent security[J]. Electronics & Communication Engineering, 2002, 14(5): 211-218.

[2] YEE B S. A Sanctuary for Mobile Agents[A]. LNCS 1603[C]. Springer-Verlag, Berlin Heidelberg, 1997. 261-273.

[3] KARJOTH G, ASOKAN N, GULCU C. Protecting the Computation Results of Free-Roaming Agents[A]. LNCS 1477[C]. Springer-Verlag, Berlin Heidelberg, 1998. 195-207.

[4] MAGGI P, SISTO R. A Configurable Mobile Agent Data Protection Protocol[A]. Proc. of the 2nd International Conference on Autonomous Agents and Multiagent Systems (AAMAS'03)[C]. Melbourne, Australia. ACM Press, New York, USA, 2003. 851-858.

[5] MING Y, KUN P, MATT H, *et al*. Using Recoverable Key Commitment to Defend Against Truncation Attacks in Mobile Agents[A]. LNCS 3182[C]. Springer-Verlag Berlin Heidelberg, 2004. 164-173.