企业内部基于移动 Agent 的 Web 页面安全电子邮件应用*

李 凯，周建国，晏蒲柳
(武汉大学 电子信息学院，湖北 武汉 430072)

摘 要：分析了当前几种广泛应用的安全电子邮件标准在安全机制方面的某些不足，该方案利用功能 Agent 在客户端和认证中心之间进行双向认证、公钥管理和邮件管理，实现了邮件的保密性、认证性、完整性以及收发双方的不可否认性。

关键词：安全邮件；移动 Agent；通信机制；认证中心
中图法分类号：TP393.08 **文献标识码**：A **文章编号**：1001-3695(2005)02-0102-03

A Mobile Agent-based Application of Web Secure E-mail in Enterprise

LI Kai, ZHOU Jian-guo, YAN Pu-liu
(School of Electronic Information, Wuhan University, Wuhan Hubei 430072, China)

Abstract: The defects of several widely applied secure E-mail standards are analyzed. This application uses functional Agent to complete bidirectional authentication, public key management and mail management between the client end and the CA, it implements the secrecy, authentication, integrality and undeniable property of E-mail.

Key words: Secure E-mail; Mobile Agent; Communication Mechanism; Certificate Authority (CA)

1 引言

随着 Internet 的迅速普及，电子邮件得到了广泛的应用，并已成为人们信息交流的重要工具，但由此也带来了很多不安全因素。比如在许多电子邮件系统中，邮件的内容都是以明文或者把明文经过某种简单可逆的编码(如 Base64 编码)处理后在网络中直接传递的，邮件被截获后，内容将暴露无遗。为了提高邮件通信的安全性，技术界先后提出了多种基于公钥加密体制的安全电子邮件标准。在这些标准中以 PGP 和 S/MIME 的应用最为广泛，许多安全电子邮件产品是基于这两种标准的。

在以公钥密码算法为基础的安全电子邮件系统中，用户身份的认证以及公钥的产生、管理、分发、撤销等环节非常重要，这些因素直接决定了系统的安全性。PGP 方案中没有设置可信赖中心来认证用户和管理公钥，而是利用链式信任网通过私人方式转介公钥。S/MIME 则是建立在公钥基础设施(PKI)基础上的一套安全邮件标准，它设有认证中心(CA)来负责生成、管理和分配公钥，但传统的 CA 权限过高，甚至可以偷窥到邮件内容。

针对上述标准中存在的问题，笔者尝试把移动 Agent 技术引入企业内部的安全电子邮件的应用中，研究设计了一套利用移动 Agent 在客户端与 CA 端之间完成双向认证、公钥管理和邮件管理等任务的应用方案。该方案中客户端邮件的收发将以 Internet Explorer 浏览器为基本平台，通过 IE 编程和移动 Agent 技术实现安全功能。

收稿日期：2004-03-05；修返日期：2004-05-21
基金项目：湖北省科技攻关项目(2003AA101C07)

2 移动 Agent 技术

与传统的 C/S 构架比较，移动 Agent 技术通过将请求某项服务的 Agent 动态地迁移到服务器端执行，使得它较少地依赖网络传输这一中间环节而直接面对要访问的服务器资源，降低了系统对网络带宽的依赖。移动 Agent 也不需要统一的调度，用户创建的 Agent 可以在不同节点上异步地运行，当任务完成以后再将结果传送给用户。为了完成某些特定任务，用户可以创建多个 Agent，也可以多个用户创建相同内容的 Agent，这些 Agent 在一个或多个节点上运行，并行求解。

移动 Agent 的这些特点，给安全电子邮件系统中公钥管理和邮件管理等功能的实现提供了新思路。另外由于多个 Agent 可以在节点上并行运行，也比较适合认证中心能够处理多个用户同时申请服务的要求。

3 移动 Agent 在安全电子邮件中的应用设计方案

3.1 整体框架和功能介绍

基于移动 Agent 的企业内部安全电子邮件系统的整体框架如图 1 所示。该系统通过客户端以及认证中心 CA 端的各种功能 Agent 之间的安全通信机制，避免了现行安全电子邮件标准的一些不足：它通过设置认证中心 CA 及公钥和邮件摘要信息数据库，避免了 PGP 中存在的公钥管理和邮件管理方面的不足；另一方面，它拥有灵活的公钥产生、上传和获取方式，在 CA 端只保存各用户的公钥，从而避免了 S/MIME 中由于

CA 拥有过高权限而导致的安全隐患。

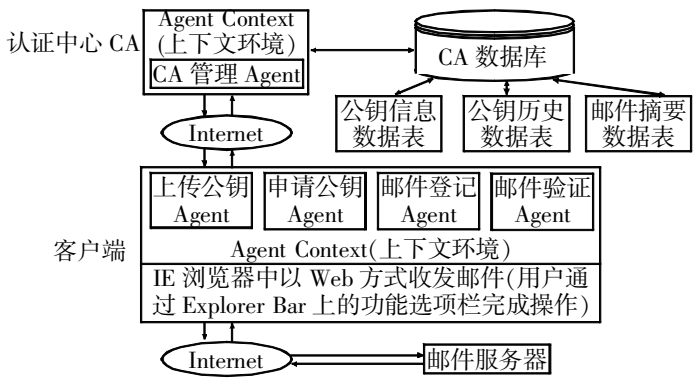

图 1　安全电子邮件系统整体框架图

该系统能够实现以下功能:

(1) 邮件保密性。邮件发送之前都要利用接收方公钥进行加密, 保证邮件以密文的形式在网络中传输, 只有通过接收方的私钥才能解密获得明文。

(2) 邮件认证性。邮件发送之前要通过发送方的私钥进行签名, 接收方通过发送方的公钥来验证签名, 并以此认证发送方的身份。

(3) 邮件完整性。邮件发出前要通过单向散列函数求出不可逆的摘要值, 并保存在 CA 端的数据库中, 接收方通过比较这个摘要值和收到的邮件的摘要值, 就能确定邮件内容在传输过程中有没有改变。

(4) 发送方不可否认性。通过 CA 端相关数据库的记载可以确认发送方确实发送了邮件, 而不用管他是否承认。

(5) 接收方不可否认性。通过 CA 端相关数据库的记载可以确认接收方确实接收并解密了邮件, 而不用管他是否承认。

3.2　认证中心 CA 端的设计

认证中心 CA 端分为前端监视程序和后端数据库两大部分。后端数据库中包括三个数据表, 分别管理用户公钥信息、公钥历史信息以及邮件摘要信息。前端监视程序则通过移动 Agent 上下文环境(Agent Context) 产生并运行 CA 管理 Agent, 这个 Agent 负责与客户端发来的各种功能 Agent 进行通信, 并相应地对后端数据库进行操作, 实现安全功能。

3.3　客户端的设计

客户端分为两大功能模块, 一部分通过 IE 编程, 以 IE 浏览器上 Explorer Bar 的形式提供给用户完成收发安全邮件和其他安全操作的接口; 另一部分则是具体完成邮件加密解密、邮件签名认证、产生上传公钥、申请获取公钥、邮件登记认证等安全功能的模块。在安全功能模块, 通过 Agent Context 产生并管理各种功能 Agent(图 1) 。根据具体需把不同的功能 Agent 发往 CA 端, 并通过相应的安全通信机制与 CA 管理 Agent 进行通信, 完成通信后携带数据回到客户端, 客户端再根据数据完成其他安全操作。

3.4　各功能移动 Agent 与 CA 管理 Agent 之间安全通信机制

客户端是通过发送功能 Agent 到 CA 端, 与 CA 管理 Agent 进行通信来完成各项安全功能的。由于通信的内容涉及到公钥、邮件摘要等重要信息, 如何保证通信的安全对于系统的安全性非常重要。笔者设计了一套各功能 Agent 与 CA 管理 Agent 之间双向认证的通信机制, 可以起到良好的安全效果。

3.4.1　上传公钥通信机制(以用户 A 上传公钥为例)

上传公钥 Agent 将携带 A 的 ID、新公钥以及 A 对新公钥的签名, 在被发往认证中心后与 CA 管理 Agent 按下列机制通信(图 2) :

(1) 上传公钥 Agent 请求上传新公钥并向 CA 管理 Agent 发送 A 的 ID、新公钥以及 A 对新公钥的签名。

(2) 管理 Agent 收到后, 首先在用户公钥表中查找 A 的 ID, 若未找到, 则返回上传者为非法用户的信息和签名。若找到, 则先用 A 的公钥验证它对新公钥的签名, 若未成功, 则返回验证签名不成功的信息和签名; 若验证成功, 则更新用户公钥表和用户公钥历史表, 并返回更新成功的信息和签名。

(3) 公钥 Agent 收到后, 验证信息和签名, 并根据不同返回信息作出不同处理: 若已经更新成功则返回客户端并确认 A 可以使用新公钥, 若更新不成功则重新发送。

3.4.2　申请公钥通信机制(以用户 A 申请用户 B 公钥为例)

申请公钥 Agent 将携带 A 的 ID, B 的邮件账号和 A 对它们的签名以及认证中心的公钥, 在被发往认证中心后与 CA 管理 Agent 按下列机制通信(图 2) :

(1) 申请公钥 Agent 请求登录并向 CA 管理 Agent 发送 A 的 ID 以及对 ID 的签名。

(2) 管理 Agent 收到后, 先通过 ID 在用户公钥表中查找 A, 取得 A 的公钥, 并验证签名。如果验证通过, 将 A 成功登录的信息和签名返回给申请公钥 Agent。

(3) 申请公钥 Agent 若没有收到成功登录信息将再次请求登录; 若收到成功登录信息则继续发送 B 的邮件账号以及 A 对账号的签名, 以请求 B 的公钥。

(4) 管理 Agent 收到后将验证签名。成功后, 在用户公钥表中通过 B 的邮件账号查找 B 的 ID 和公钥, 并把 B 的 ID 和公钥以及 CA 对它们的签名发给申请公钥 Agent。

(5) 申请公钥 Agent 验证签名后将携带 B 的 ID 和公钥返回客户端, 由加密模块利用这个公钥完成对 AES 密钥(明文已用此 AES 密钥加密) 的加密。

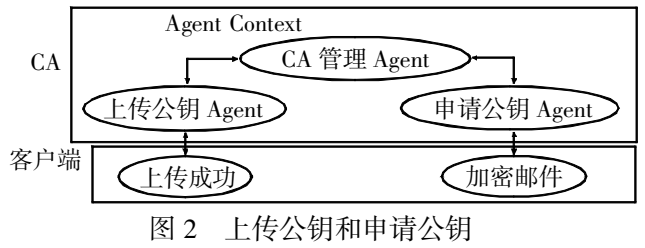

图 2　上传公钥和申请公钥

3.4.3　邮件登记通信机制(以用户 A 向用户 B 发送邮件并登记为例)

邮件登记 Agent 将携带 A 的 ID、B 的 ID、邮件的摘要值和 A 对它们的签名以及认证中心的公钥, 在被发往认证中心后与 CA 管理 Agent 按下列机制通信(图 3) :

(1) 邮件登记 Agent 把邮件明文的摘要及 A 对摘要的签名发给 CA 管理 Agent。

(2) CA 管理 Agent 在对签名验证成功后, 在邮件摘要表中记录邮件摘要及 A 的签名, 并向邮件登记 Agent 返回摘要的编号及 CA 对编号的签名。

(3) 邮件登记 Agent 验证签名成功以后将携带获得的邮件摘要编号返回客户端。客户端将密文、用 B 的公钥加密过的 AES 密钥以及明文摘要的编号一起发送到 B 的邮箱所在的邮

件服务器。

3.4.4 邮件验证通信机制(以用户 B 收到用户 A 发来的邮件并验证为例)

客户端在收取邮件以后将解析正文各部分内容,并首先验证 CA 对 A 的公钥和摘要编号的签名,若失败,则记录失败信息。然后用 A 的公钥验证 A 对加密后的 AES 密钥的签名,若失败,则记录失败信息。如果以上验证都成功,则用 B 的私钥解密 AES密钥,并用这个密钥解密邮件密文得到明文 N,对 N 求得摘要值。

邮件验证 Agent 将携带 B 的 ID、原明文摘要的编号和 B 对它们的签名以及解密明文 N 的摘要值,在被发往认证中心后与 CA 管理 Agent 按下列机制通信(图 3):

(1) 邮件验证 Agent 向 CA 管理 Agent 请求原明文的摘要。

(2) CA 管理 Agent 通过 B 的 ID 在用户公钥表中获得 B 的公钥,验证 B 的签名,成功以后利用摘要编号在摘要信息表中获得原来存储的摘要,并返回给邮件验证 Agent。

(3) 邮件验证 Agent 将获得的摘要值与解密明文摘要值进行比较,如果匹配说明邮件在传输过程中没有被改变,向 CA 管理 Agent 发送验证成功信息,并返回客户端。此时客户才可以看到经过解密并验证确认的邮件。

(4) CA 管理 Agent 则在邮件摘要信息表中,记录邮件接收解密验证成功。

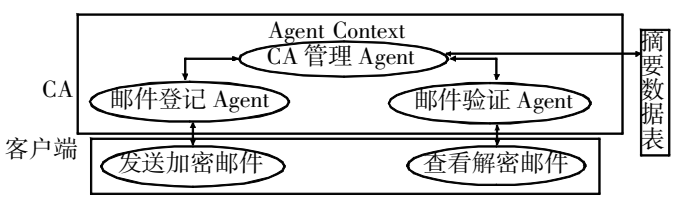

图 3 邮件登记和邮件验证

4 系统安全性分析与客户端界面实现

4.1 移动 Agent 系统安全性分析

本方案中采用移动的 Agent 系统是日本 IBM 公司开发的 Aglet。Aglet 系统的安全框架可定义多种安全策略。这里的安全策略是一个由管理者定义的规则集,它包括 Aglet 在什么情况下可以访问对象,用户请求的认证及认证的实体所允许执行的操作,Aglet 之间及与上下文环境(Context)之间的通信安全要求等。

Aglet 服务器使用 JDK(Java. Security. SecureRandom)提供的伪随机种子产生算法用于服务器的认证,完整性、私密性检查,登录口令的产生。

4.2 通信机制安全性分析

在本方案的安全通信机制中,发送方在发送邮件之前,要把邮件的摘要及其签名通过邮件登记 Agent 发到 CA 备份。接收方解密获得明文后,也要求出摘要值并随邮件验证 Agent 发往 CA 进行验证。而且,只有验证成功,邮件验证 Agent 才能返回客户端并允许客户查看解密的明文。这样,CA 就同时保存发送方对原始邮件摘要的签名以及接收方解密验证成功的记录,这是实现收发双方不可否认性的关键,而传统的安全电子邮件系统缺少这项重要的安全功能。

通常在基于 CA 的认证协议中,CA 权利过大,用户的公私密钥对都是由它产生的,它有可能偷看到用户的加密邮件。在本方案中,设计了一种公钥上传机制,即可由用户自己产生密钥对,然后通过上传公钥 Agent 上传公钥,这样私钥就只有用户自己知道,即使 CA 也无法读取用户的加密邮件。这种做法既吸取了传统 CA 的优点,又摒弃了不足,增强了系统的安全性。

4.3 客户端 Web 页面实现

当用户启动 IE 浏览器后,点击“查看/浏览器栏/Secure Mail”下的相关菜单项,就会在浏览器底部出现加密、签名、公钥管理等功能选项栏,如图 4 所示。

图 4 客户端 Web 页面

5 结束语

本文在分析了 PGP 和 S/MIME 这两种安全电子邮件不足的基础上,研究设计了一套适合企业内部使用的 Web 页面安全电子邮件系统应用方案。该方案利用移动 Agent 技术的移动性与自主性在客户端与认证中心 CA 端之间进行双向认证通信,实现了邮件的保密性、认证性、完整性,尤其是邮件收发双方的不可否认性等功能。

参考文献:

[1] illiam Stallings. 网络安全要素——应用与标准[M]. 北京:人民邮电出版社,2000.

[2] Scott Roberts. Internet Explorer 5 程序设计[M]. 北京:清华大学出版社,2001.

[3] 王育民,刘建伟. 通信网的安全——理论与技术[M]. 西安:西安电子科技大学出版社,1999.

[4] 张云勇,刘锦德. 移动 Agent 技术[M]. 北京:清华大学出版社,2003.

[5] Messaoud Benabtar. 互联网公钥基础设施概论[M]. 张千里,等. 北京:人民邮电出版社,2003.

[6] Linn J. Privacy Enhancement for Internet Electronic Mail-Part Ⅰ: Message Encryption and Authentication. Procedures RFC 1421[EB/OL]. http://www.rfc-editor.org, 2001-08.

[7] Kent S. Privacy Enhancement for Internet Electronic Mail-Part Ⅱ: Certificate-based Key Management RFC 1422[EB/OL]. http://www.rfc-editor.org, 2001-08.

[8] Balenson D. Privacy Enhancement for Internet Electronic Mail-Part Ⅲ: Algorithms, Modes and Identifiers RFC 1423[EB/OL]. http://www.rfc-editor.org, 2001-08.

[9] Kaliski B. Privacy Enhancement for Internet Electronic Mail-Part Ⅳ: Key Certificate and Related Services RFC 1424[EB/OL]. http://www.rfc-editor.org, 2001-08.

作者简介:

李凯(1980-),男,湖北人,硕士研究生,研究方向为计算机网络与信息安全;周建国(1965-),男,湖北人,副教授,硕士,研究方向为计算机网络;晏蒲柳(1962-),女,湖北人,教授,博士生导师,博士,研究方向为计算机网络。