

[19] 中华人民共和国国家知识产权局



[12] 发明专利申请公布说明书

[21] 申请号 200810105592.8

[51] Int. Cl.

H04L 12/58 (2006.01)

H04L 29/06 (2006.01)

[43] 公开日 2009 年 11 月 4 日

[11] 公开号 CN 101572678A

[22] 申请日 2008.4.30

[21] 申请号 200810105592.8

[71] 申请人 北京明朝万达科技有限公司

地址 100085 北京市海淀区安宁庄西路 9 号
院 29 号楼 1201

[72] 发明人 喻 波 李志涛 顾 飞 罗 捷
谢湘宁 王志海

权利要求书 2 页 说明书 7 页 附图 2 页

[54] 发明名称

一种邮件附件透明保密控制方法

[57] 摘要

在网络盛行的今天，电子邮件越来越普及，是网络时代最方便的交流方式，省钱、快捷。通过电子邮件传送信息，一般人都认为很安全。事实上在网络上传输的数据是不加密的，网络的自由性使邮件的安全问题日益突出，第三者会轻易获知邮件的内容。要解决这些问题，目前最好的办法是对电子邮件进行加密。本发明邮件智能加密，实现对本地客户端发送邮件的附件进行加密，用户在特定的授权客户端使用私钥对邮件解密才可阅读邮件附件内容。传送邮件时，假如没有相应的私人秘钥，邮件附件内容只会是一片无法阅读的乱码。所以，即便在公共密钥公开的情况下，除非客户端用户拥有私钥，否则邮件附件信息及内容是加密不可见的，而发件人授权的收件人是拥有私钥的唯一合法人选。实现对单位信息网络中核心数据的监控和保密，从而防止数据泄密。

1、一种邮件附件透明保密控制方法，其特征在于：采用包括对网络、邮件发送端、邮件接收端、数据存储和数据交换等的综合控制技术，实现通用的防止邮件附件数据泄密的目标。

2、如权利要求1所述的一种邮件附件透明保密控制方法，其特征在于：通过对POP3/SMTP协议附件和Web附件的分析和提取，结合加密技术，在授权的计算机上使用密钥自动加密/解密，实现邮件附件的透明保密控制。

3、如权利要求1或2所述的一种邮件附件透明保密控制方法，其特征在于：通过邮件智能加密编码技术和还原重编码技术，使邮件从加密发送和解密接收完全实现，在此基础上还使用特殊客户端概念，将加密技术构架在一个特殊平台上，区别以往简单端到端的普通邮件加解密，达到了智能邮件加密的效果。

4、如权利要求1或2所述的一种邮件附件透明保密控制方法，其特征在于：使用邮件标题、附件加密识别技术，它的核心是加密标记技术。使用此技术在邮件标题或附件字符串的字头添加标记，表示该邮件是加密邮件，提高判断邮件是否加密的解析过程效率。

5、如权利要求1或2所述的一种邮件附件透明保密控制方法，其特征在于：使用黑名单技术和白名单技术，客户端在进行邮件加密时使用黑白名单技术使邮件发送接收行为受到控制。

6、利用权利要求3所述的一种邮件附件透明保密控制方法，其特征在于：实施加密的邮件附件，在特定客户端的策略下由发件者使用公钥加密，在相同的特定客户端授权收件者使用私钥对邮件解密直接阅读，而在普通客户端收件人需要使用特定的察看工具和私钥解密察看加密邮件，未经特殊授权的用户不能通过普通方式察看机密邮件附件。

7、利用权利要求4所述的一种邮件附件透明保密控制方法，其特征在于：客户端在对邮件加密的过程中应用字符串模式匹配，在邮件标题或附件字符串的字头添加标记，表示该邮件是加密邮件，接收端收邮件时对标头进行识别，确定是加密邮件后主要针对收件人邮箱地址字符串进行的匹配，若匹配成功即

识别并确认邮件是正确接收的可解密的邮件，否则抛弃邮件不予解析。

8、利用权利要求 5 所述的一种邮件附件透明保密控制方法，其特征在于：黑名单技术，设定电子邮件发送控制的动作缺省“允许”，再设定禁止的接收邮件者；白名单技术，设定电子邮件发送控制的动作缺省值为“禁止”，再设定允许的接收邮件者，实现了邮件发送接收行为的灵活设置和应用，客户端可依据实际情况选择较优的方案，提高工作者的效率。

9、如权利要求 1 或 2 所述的一种邮件附件透明保密控制方法，其特征在于：实现了邮件附件保密的基础功能，在此基础上还实现了邮件标题和正文的加密。邮件的加密可以按照不同接收者的地址设置不同环境下的加密，实现多条件下邮件加密。

一种邮件附件透明保密控制方法

技术领域

本发明的目的在于通过对 POP3/SMTP 协议附件和 Web 附件的分析和提取，结合加密技术，在授权的计算机上使用密钥自动加密/解密，实现邮件附件的透明保密控制。

背景技术

随着计算机技术和通信技术的飞速发展，电子邮件作为当前和未来网络使用者的主要沟通方式，它的地位越来越重要。电子邮件的使用不可避免的涉及到大量敏感信息，这就有了安全隐患，所以信息系统中防止邮件数据泄密已经成为一个关注的焦点，也是企事业单位进行数字知识产权保护需要采取的必要手段。现有的防止邮件泄密的技术，主要采用端到端的安全电子邮件加密技术，这种方法从个人主观意愿出发，实现起来比较容易，采用简单的密码技术即可实现。

本发明邮件附件透明保密技术从单位管理者的角度出发，要防止单位内部任何能够接触到涉密数据的人员有意或者无意将泄密数据以邮件方式泄密的发生，从而实现对单位数字知识产权的保护和保密。

现有的邮件加密技术，都仅单一采用了部分技术措施，难以实现全面的强制防止邮件泄密的效果。典型的包括只对普通用户进行端到端的邮件加密控制，但是对特殊用户邮件就没有办法控制；还有通过网络协议内容过滤的方式防止数据泄密，但是如果数据经过加密/压缩等简单处理，则无法防止；再有就是对正文类型文件采用加密措施，但是无法防止附件文件格式转换和内存数据复制带来的数据泄密漏洞。本发明所描述的邮件附件透明保密控制方法，主要使用

邮件发送监控、邮件接收监控、邮件智能加密等方法实现。

专利发明内容

本发明基于邮件加密密钥的基础上，通过定义不同客户端不同工作环境的模式，结合邮件发送监控、邮件接收监控、邮件智能加密等综合技术方案，实现对单位信息网络中核心数据的监控和保密，从而防止数据泄密。

本发明实现的时候，需要对实施邮件加密的客户端的工作环境进行设置，即需要判断和确定不同的工作模式和服务器是否连接的情况下，控制需要加密邮件的加密情况。实施加密的邮件附件，在特定客户端的策略下由发件者使用公钥加密，在相同的特定客户端授权收件者使用私钥对邮件解密直接阅读，而在普通客户端收件人需要使用特定的察看工具和私钥解密察看加密邮件，未经特殊授权的用户不能通过普通方式察看机密邮件附件。

本发明采用的综合控制技术，将以管理策略的形式来表现，根据每个具体工作环境的需要，管理者可以进行灵活的定义。

本发明中邮件加密技术的核心是智能加密编码识别技术和还原重编码技术。智能加密编码技术应用在邮件加密流程中，邮件加密端使用特定的加密密钥将邮件编码加密，实现特定客户端邮件附件的加密发送；还原重编码技术应用在邮件解密的流程中，加密邮件存放在服务器中，并通过内、外网络发包表示邮件已经加密发送，邮件的授权接收用户通过网络接收并确认包的信息，将邮件存放在服务器中，特定客户端将使用授权的私钥对邮件解析在客户端上，此时指定的接收者可以直接读取机密邮件，在普通客户端使用私钥解析邮件后需要特殊的查看工具读取加密邮件。

通过邮件智能加密编码技术和还原重编码技术，使邮件从加密发送和解密接收完全实现，在此基础上还使用特殊客户端概念，将加密技术构架在一个特殊平台上，区别以往简单端到端的普通邮件加解密，达到了智能邮件加密的效果。

本发明中邮件标题、附件加密识别技术的核心是加密标记技术。加密标记技术应用在加密、解密邮件的流程中。客户端在对邮件加密的过程中应用字符串模式匹配，在邮件标题或附件字符串的字头添加标记，表示该邮件是加密邮件，接收端收邮件时对标头进行识别，确定是加密邮件后主要针对收件人邮箱地址字符串进行的匹配，若匹配成功即识别并确认邮件是正确接收的可解密的邮件，否则抛弃邮件不予解析。

通过加密标记技术，使邮件解析过程效率提高。

本发明中邮件加密控制技术的核心技术是黑名单技术和白名单技术。黑名单和白名单是互斥的，只能单独设置黑名单或者白名单。客户端在进行邮件加密时使用黑白名单技术使邮件发送接收行为受到控制。

黑名单技术，设定电子邮件发送控制的动作缺省“允许”，即默认所有的接收者都允许接收加密邮件，再设定禁止的接收邮件者，实现除了设定的关键收件人外，其他均不进行管理；白名单技术，设定电子邮件发送控制的动作缺省值为“禁止”，即默认所有接收者都禁止接收加密邮件，再设定允许的接收邮件者，实现除了设定的关键收件人允许外，其他均不允许使用。

黑白名单技术，实现了邮件发送接收行为的灵活设置和应用，客户端可依据实际情况选择较优的方案，提高工作者的效率。

本发明所描述的邮件附件透明保密控制方法，主要使用邮件发送监控、邮件接收监控、邮件智能加密等方法实现。当前设计针对 POP3/SMTP 协议附件和 Web 附件的分析和提取，通过设置生效和例外邮件地址来控制是否进行发送、接收监控和智能加密。

1、 邮件发送监控

本发明邮件发送监控通过对收件人邮件地址的定义，实现在审计日志中记录所发邮件的信息及内容。

邮件发送监控功能描述如下：

- 1) 通过黑白名单的方式设置用户使用 POP3/SMTP 协议和 Web 发送邮件的权

-
- 限，对客户端所发邮件进行监控；
 - 2) 实现客户端在不同工作环境下设置邮件监控；
 - 3) 实现多收件人的邮件监控。

邮件发送监控的流程如图 1 所示，描述如下：

- 1) 通过黑白名单的方式设置客户端的工作条件，添加收件人邮件地址；
- 2) 使用 POP3/SMTP 协议或 Web 发送邮件，服务器记录邮件信息；
- 3) 在审计日志中查阅受监控邮件的信息和内容。

2、邮件接收监控

本发明邮件接收监控通过对发件人邮件地址的定义，实现在审计日志中记录所接收邮件的信息及内容。

邮件接收监控功能描述如下：

- 1) 通过黑白名单的方式设置用户使用 POP3/SMTP 协议和 Web 接收邮件的权限；
- 2) 实现客户端在不同工作环境下设置邮件监控；
- 3) 实现多发件人的邮件监控。

邮件发送监控的流程如图 2 所示，描述如下：

- 1) 通过黑白名单的方式设置客户端的工作条件，添加发件人邮件地址；
- 2) 使用 POP3/SMTP 协议或 Web 发送邮件，服务器记录邮件信息；
- 3) 在审计日志中查阅受监控邮件的信息和内容。

3、邮件智能加密

本发明邮件智能加密通过对收件人邮件地址的定义，实现对发送邮件附件内容加密的功能。并在审计日志中记录被加密邮件的信息及内容。

邮件智能加密功能描述如下：

- 1) 通过黑白名单的方式设置用户使用 POP3/SMTP 协议和 Web 接收邮件的权

限；

- 2) 实现客户端在不同工作环境下对发送邮件进行加密；
- 3) 邮件智能加密实现针对邮件正文和附件的加密，实现针对 Base64、Quoted-Printable、7Bit 和 8Bit 附件编码的加解密支持；
- 4) 实现多发件人的邮件监控。

邮件智能加密的流程如图 3 所示，描述如下：

- 1) 通过黑白名单的方式设置客户端的工作条件，添加收件人邮件地址；
- 2) 使用 POP3/SMTP 协议或 Web 发送邮件，在客户端对邮件使用公钥进行加密随后放到服务器上准备发送，服务器同时记录邮件信息；
- 3) 接收方在特定客户端根据自身邮件地址生成的私钥来解密；
- 4) 在审计日志中查阅加密邮件的附件信息和内容。

为使发明具有更严密的完整性，本发明在技术方面还将有下列后续补充。

当前设计将针对 Smtp 和 Pop3 协议的邮件发送、接收监控和邮件智能加密的规则合并为一个规则邮件管理功能进行处理，通过设置生效和例外邮件地址来控制是否进行发送、接收监控和智能加密。

智能加密使用属性页控制加密操作，进行加密审计和邮件内容审计，将智能加密控制分为普通模式邮件加密（时间密钥）、VCN 域模式邮件加密和 DMS 模式邮件加密，加密格式包括：标题加密、正文加密和附件加密。

普通模式邮件加密以时间密钥种子进行邮件加密发送控制，默认在安装了客户端的邮件都有邮件智能解密功能。

域模式邮件加密以域信息密钥进行邮件加密发送控制，设置接收方式从而控制同域、信任域和全部接收自动解密功能。

DMS 模式邮件加密以 DMS 模式信息密钥进行邮件加密发送控制，设置接收方式从而控制相同加密等级、低加密等级接收自动解密功能。

邮件管理规则下发到客户端之后，当和可信系统中独立的邮件发送控制规则、接收控制规则和邮件智能加密规则同时存在时，以邮件管理规则为优先。当没有邮件管理规则时，以原有的处理方式为准。

以上是本发明后继会增加的功能，使邮件保密系统得到最大程度的完善。

附图说明

图 1A 和图 1B 为本发明中使用邮件加密的技术原理图；

图 1C 为本发明中使用标题、附件加密识别的技术原理图；

图 1D 为本发明中使用邮件加密控制技术的原理图；

图 1 为邮件发送监控的流程示意图；

图 2 为邮件接收监控的流程示意图；

图 3 为邮件智能加密的流程示意图。

具体实施方式

1. 安装文件网络外发控制的环境

由厂家提供安装程序。

2. 管理员授权可以使用此发明的客户端权限

根据用户数量，按厂家提供的授权功能进项操作（添加到系统中）。可根据用户的特点，如组织机构等，将用户划分成不同的用户组进行不同的权限控制。

3. 设置邮件只能加密的各项控制条件

1) 设置受控客户端的不同工作环境；

2) 按照收件人的邮件地址确定要发送给此地址的邮件都加密；

3) 选择白名单或黑名单的控制方法；

4、实施邮件智能加密策略

在客户端实施邮件智能，注意设置客户端上邮件加密实施的工作环境，

各工作环境之间是相互独立实施邮件加密，高效实现邮件附件数据隐藏技术。

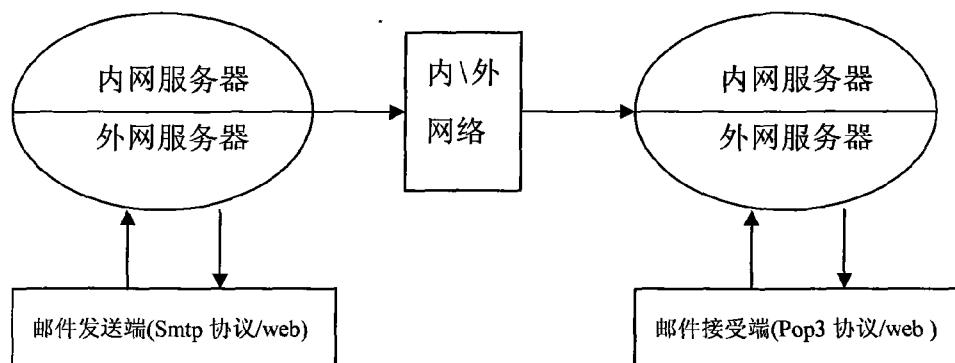


图 1A



图 1B

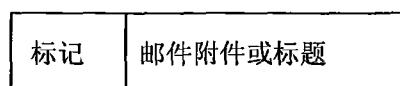


图 1C

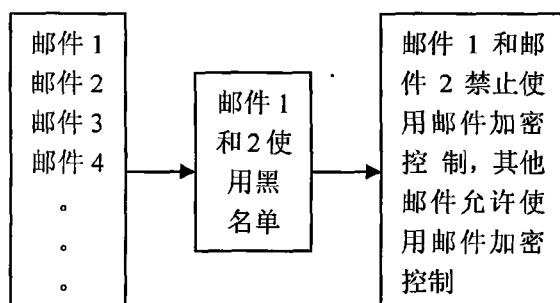


图 1D (a)

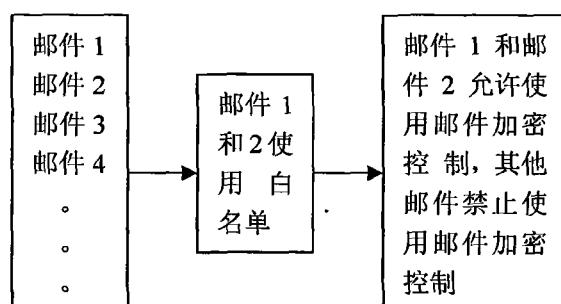


图 1D (b)

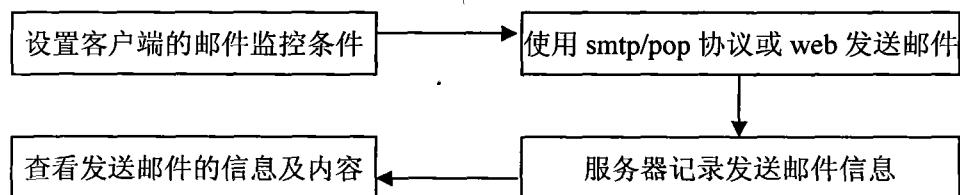


图 1

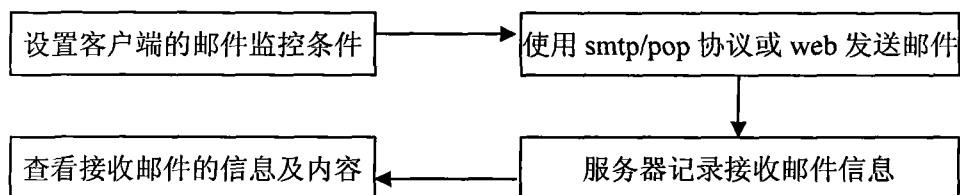


图 2

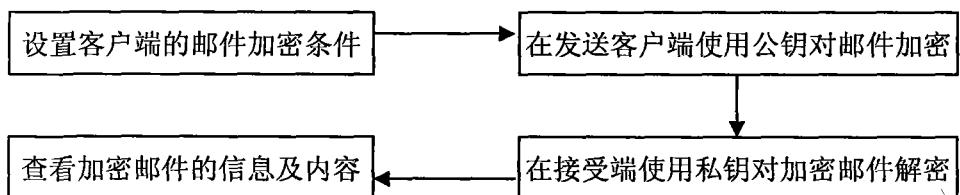


图 3