

(19) 中华人民共和国国家知识产权局



(12) 发明专利

(10) 授权公告号 CN 102999732 B

(45) 授权公告日 2015.04.22

(21) 申请号 201210483076.5

(22) 申请日 2012.11.23

(73) 专利权人 富春通信股份有限公司

地址 350003 福建省福州市鼓楼区铜盘路软件大道 89 号 C 区 25 号楼

(72) 发明人 林文美 缪品章 翁鲲鹏 王美方演

(74) 专利代理机构 福州市鼓楼区博深专利代理事务所(普通合伙) 35214

代理人 林志峰

(51) Int. Cl.

G06F 21/62(2013.01)

(56) 对比文件

CN 1928881 A, 2007.03.14, 全文.

EP 2006792 A2, 2008.12.24, 全文.

CN 100449560 C, 2009.01.07, 全文.

US 2010306534 A1, 2010.12.02, 全文.

审查员 赵洋

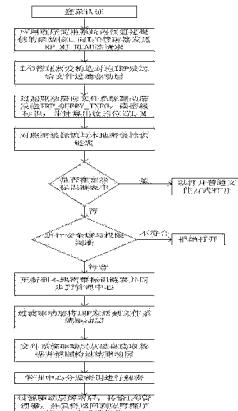
权利要求书4页 说明书7页 附图2页

(54) 发明名称

基于信息密级标识的多级域防护方法及系统

(57) 摘要

本发明提供了一种基于信息密级标识的多级域防护方法及系统，通过基于包括创建者标识、文件标识及域安全级别标识的密级标识实现对涉密文件的动态加密 / 解密，从而实现合法用户的细粒度访问，解决不同密级的信息从生成 - 访问 - 流通 - 销毁这一系列过程中所存在的信息泄露威胁。



1. 一种基于信息密级标识的多级域防护方法,其特征在于:通过在内核操作系统的驱动框架的 I/O 管理器与文件系统驱动层之间嵌入文件系统过滤层以执行包括,通过认证用户创建密文,

包括在收到写的 I/O 请求包请求后,向文件系统驱动层发送写的 I/O 请求包请求,从而在待加密文件中加入密级标识再通过加密算法加密后将其以密文形式保存的步骤;其中,所述密级标识包括有创建者标识、文件标识及域安全级别标识,所述域安全级别标识与创建用户所在域相对应,所述创建者标识与创建用户的权限级别相对应;

用户访问密文,包括,

主动提取待访问密文的密级标识与访问用户的权限比较,仅当密级标识与访问用户的权限匹配时向文件系统驱动层发送读的 I/O 请求包请求读取密文然后解密的步骤;

密文流通控制,包括,

多级域信息流向控制,当密文在多级域中流通时,通过劫持密文然后根据访问策略比较密文的密级标识中的域安全级别标识是否高于当前流通域,高于则对密文执行拦截,否则对密文执行放行 / 转发的步骤;

同级域信息流向控制,当密文在同一级域中流通时,通过劫持密文然后根据访问策略比较密文的密级标识中的创建者标识是否高于接收用户,是则对密文执行拦截,否则对密文执行放行 / 转发的步骤;

用户行为审计,包括,

根据密文的密级标识中文件标识为身份标识进行用户行为的日志审计与危险操作下发出报警的步骤。

2. 如权利要求 1 所述的基于信息密级标识的多级域防护方法,其特征在于:所述通过认证用户创建密文具体包括步骤,

A1)、通过页面重定向,强制用户通过 SSL 安全机制实现握手认证,建立通信安全通道,连接服务端;

A2)、用户端调用操作系统读写信息函数向 I/O 管理器发送写请求;

A3)、I/O 管理器提取包括进程名称、存储路径、开始地址、数据长度、待存储数据的构造写请求对应的 I/O 请求包,并将该 I/O 请求包发送到文件系统过滤层;

A4)、文件系统过滤层收到数据包后,主动向文件系统驱动层发送一次 I/O 请求包的写请求,请求在待加密文件的文件头加入密级标识,同时对应用户创建密级标识链表用于保存上述密级标识,并将密级标识链表更新至服务端,根据密级标识中的加密算法完成加密;

A5)、文件系统过滤层将加密后的 IRP 数据包发送给文件驱动系统,并最终将带有密级标识的涉密信息以密文形式保存。

3. 如权利要求 2 所述的基于信息密级标识的多级域防护方法,其特征在于:所述用户访问密文具体包括步骤,

B1)、通过页面重定向,强制用户通过 SSL 安全机制实现握手认证,建立通信安全通道,连接服务端;

B2)、用户端应用程序调用系统内核组建提供的函数接口向 I/O 管理器发送读请求;

B3)、I/O 管理器提取包括进程名称、存储路径、开始地址、数据长度的构造读请求对应

的 I/O 请求包，并将该 I/O 请求包发送到文件系统过滤层，等待读取返回的密文；

B4)、文件系统过滤层向文件系统驱动层发送密级标识读取指令，获取本次访问密文的密级标识；

B5)、将密级标识中的文件标识与用户的密级标识链表对比，若密级标识链表中已有，则继续步骤，若无，则进行权限的对比，若创建者标识高于接收用户权限则返回错误，否则将此密文更新到密级标识链表并同步到服务端然后继续步骤；

B6)、文件系统过滤层将 I/O 请求包发送给文件系统驱动层；

B7)、文件系统驱动层接收到数据后将本次访问密文读出并返回给文件系统过滤层；

B8)、文件系统过滤层接收到返回的密文后，按照密级标识中的加密算法解密，并将解密后的数据传给 I/O 管理器；

B9)、I/O 管理器将解密后的数据传给用户端应用程序接口，完成读请求。

4. 如权利要求 1 所述的基于信息密级标识的多级域防护方法，其特征在于：所述密文流通控制中多级域信息流向控制进一步包括步骤，

C1)、比较密文的密级标识中的域安全级别标识与当前流通域的安全级别高低，高则执行拦截，否则继续步骤；

C2)、判断接收用户是否是拥有访问该密文的权限，是则继续步骤，否则返回错误；

C3)、对密文执行放行 / 转发。

5. 如权利要求 1-4 任意一项所述的基于信息密级标识的多级域防护方法，其特征在于：所述加密算法采用密钥加密，所述创建密文与访问密文中的加密、解密的密钥由服务端分发。

6. 一种基于信息密级标识的多级域防护的系统，其特征在于：通过在内核操作系统的驱动框架的 I/O 管理器与文件系统驱动层之间嵌入文件系统过滤层，文件系统过滤层包括：

通过认证用户创建密文模块，用于在收到写的 I/O 请求包请求后，向文件系统驱动层发送写的 I/O 请求包请求，从而在待加密文件中加入密级标识再通过加密算法加密后将其以密文形式保存；

上述加密算法包括在密级标识中，密级标识还包括有创建者标识、文件标识及域安全级别标识，所述域安全级别标识与创建用户所在域相对应，所述创建者标识与创建用户的权限级别相对应；

用户访问密文模块，包括主动提取待访问密文的密级标识与访问用户的权限比较，仅当密级标识与访问用户的权限匹配时向文件系统驱动层发送读的 I/O 请求包请求读取密文然后解密；

密文流通控制模块，包括，

多级域信息流向控制单元，用于当密文在多级域中流通时，通过劫持密文然后根据访问策略中的比较密文的密级标识中的域安全级别标识是否高于当前流通域，高于则对密文执行拦截，否则对密文执行放行 / 转发；

同级域信息流向控制单元，用于当密文在同一级域中流通时，通过劫持密文然后根据访问策略比较密文的密级标识中的创建者标识是否高于接收用户，是则对密文执行拦截，否则对密文执行放行 / 转发；

用户行为审计模块,用于根据密文的密级标识中文件标识为身份标识进行用户行为的日志审计与危险操作下发出报警。

7. 如权利要求 6 所述的基于信息密级标识的多级域防护的系统,其特征在于:所述通过认证用户创建密文模块具体包括,

通信连接单元,用于通过页面重定向,强制用户通过 SSL 安全机制实现握手认证,建立通信安全通道,连接服务端然后转到写请求单元;

写请求单元,用于当用户端调用操作系统读写信息函数向 I/O 管理器发送写请求;

写请求反馈单元,用于当收到写请求单元的写请求后, I/O 管理器提取包括进程名称、存储路径、开始地址、数据长度、待存储数据的构造写请求对应的 I/O 请求包,并将该 I/O 请求包发送到文件系统过滤层;

密文创建单元,用于文件系统过滤层收到数据包后,主动向文件系统驱动层发送一次 I/O 请求包的写请求,请求在待加密文件的文件头加入密级标识,同时对应用用户创建密级标识链表用于保存上述密级标识,并将密级标识链表更新至服务端,根据密级标识中的加密算法完成加密;

密文处理单元,用于当密文创建单元完成加密后,文件系统过滤层将加密后的 IRP 数据包发送给文件驱动系统,并最终将带有密级标识的涉密信息以密文形式保存。

8. 如权利要求 6 所述的基于信息密级标识的多级域防护的系统,其特征在于:所述用户访问密文模块具体包括,

通信连接单元,用于通过页面重定向,强制用户通过 SSL 安全机制实现握手认证,建立通信安全通道,连接服务端然后转到读请求单元;

读请求单元,用于当用户端应用程序调用系统内核组建提供的函数接口向 I/O 管理器发送读请求;

读反馈单元,用于当收到读请求单元的读请求后, I/O 管理器提取包括进程名称、存储路径、开始地址、数据长度的构造读请求对应的 I/O 请求包,并将该 I/O 请求包发送到文件系统过滤层,等待读取返回的密文然后转至密级标识获取单元;

密级标识获取单元,用于文件系统过滤层向文件系统驱动层发送密级标识读取指令,获取本次访问密文的密级标识;

密级识别单元,用于在密级标识获取单元获取密文的密级标识后,将密级标识中的文件标识与用户的密级标识链表对比,若密级标识链表中已有,则继续步骤,若无,则进行权限的对比,若创建者标识高于接收用户权限则返回错误,否则将此密文更新到密级标识链表并同步到服务端然后转到文件系统过滤层请求单元;

文件系统过滤层请求单元,用于文件系统过滤层将 I/O 请求包发送给文件系统驱动层;

文件系统过滤层响应单元,用于在收到文件系统过滤层请求单元的 I/O 请求包后,文件系统驱动层将本次访问密文读出并返回给文件系统过滤层;

I/O 管理器请求单元,用于在文件系统过滤层响应单元返回密文后,文件系统过滤层接收到返回的密文,按照密级标识中的加密算法解密,并将解密后的数据传给 I/O 管理器;

I/O 管理器响应单元,用于在 I/O 管理器请求单元解密密文后,由 I/O 管理器将解密后的数据传给用户端应用程序接口,完成读请求。

9. 如权利要求 6-8 任意一项所述的基于信息密级标识的多级域防护的系统，其特征在于：所述加密算法采用密钥加密，所述创建密文与访问密文中的加密、解密的密钥由服务端分发。

基于信息密级标识的多级域防护方法及系统

技术领域

[0001] 本发明涉及计算机安全技术领域,尤其是指一种基于信息密级标识的多级域防护方法及系统。

背景技术

[0002] 社会的信息化,给大家带来便捷的同时,也带来了众多安全威胁。出于安全考虑,涉密网络通常按照不同的密级进行安全域划分,按照国家要求,必须采取可靠技术,严禁高密级信息流向低密级域。而在企业内网中所涉及的众多商业机密,也需要控制在最小的知悉范围,防止信息泄露。基于密级标识的安全域管理和信息流向控制是解决该问题的方向与关键。目前在多级安全域领域,尚无完善的技术可以完美解决该问题,但在可信计算机数据安全以及文件加密等相关领域获采用了文件系统过滤驱动技术来保障数据安全。

[0003] 例如,一申请号为 200610096441.1,名称为“一种计算机数据安全防护方法”的中国发明专利就公开了一种利用微软内核操作系统的驱动框架,采用改进型文件系统过滤驱动技术,将文件过滤驱动模块嵌入到 I/O 管理器和文件系统驱动层模块之间,通过电子钥匙中的密钥和用户登录密码来确认登录用户的合法性,然后 I/O 管理器将数据包传输到文件过滤驱动模块,进行加解密认证处理,再转交到文件系统驱动层模块,从而实现对于合法用户完全透明的计算机数据安全防护。

[0004] 缺点 1 :该发明单纯的应用于计算机数据安全保护,无法实现细粒度控制,没有实现对不同密级的信息分级保护,造成只要有电子钥匙的用户均能访问各种级别的涉密信息。

[0005] 缺点 2 :没有实现对信息在多级安全域流通过程中的信息监控、拦截,更没有提供实时监控报警装置,来防止信息泄露。

[0006] 缺点 3 :没有实现用户行为的审计,对于信息泄露事故,将无法进行审计,从而无法实现责任制。

发明内容

[0007] 本发明的目的在于克服了上述缺陷,提供一种基于信息密级标识的多级域防护方法及系统。

[0008] 本发明的目的是这样实现的 :

[0009] 本发明的有益效果在于基于包括创建者标识、文件标识及域安全级别标识的密级标识实现对涉密文件的动态加密 / 解密,从而实现合法用户的细粒度访问,解决不同密级的信息从生成 - 访问 - 流通 - 销毁这一系列过程中所存在的信息泄露威胁。

附图说明

[0010] 下面结合附图详述本发明的具体结构

[0011] 图 1 为本发明的体系框架以及组成模块 ;

- [0012] 图 2 为本发明的通过认证用户创建密文的具体流程示意图；
- [0013] 图 3 为本发明的用户访问密文的具体流程示意图；
- [0014] 图 4 为本发明的密文流通控制的具体流程示意图。

具体实施方式

[0015] 为详细说明本发明的技术内容、构造特征、所实现目的及效果，以下结合实施方式并配合附图详予说明。

[0016] 本发明提供了一种基于信息密级标识的多级域防护方法，通过在内核操作系统的驱动框架的 I/O 管理器与文件驱动系统层之间嵌入文件系统过滤层以执行包括，

- [0017] 通过认证用户创建密文：

[0018] 包括在收到写的 I/O 请求包的请求后，向文件系统驱动层发送写的 I/O 请求包 (IRP-I/O Request Packet) 的请求，从而在待加密文件的中(例如通常最方便的是在文件头)加入密级标识(最佳的是一个拥有固定长度的密级标识)再通过加密算法加密后将其以密文形式保存在物理磁盘上的步骤，本步骤实现了动态透明加密。

[0019] 上述加密算法包括在密级标识中，密级标识还应当至少包括有创建者标识、文件标识及域安全级别标识，所述域安全级别标识与创建用户自身所在域相对应，所述创建者标识与创建用户自身的权限级别相对应。

[0020] 上述创建者标识以创建时间命名，如此的好处是使得创建者标识在作为文件标识的同时也明确了文件的创建时间。

[0021] 最佳的，密级标识包括文件标识 (ID 标识)、创建者标识、修改者标识、最后读取者标识，权限信息标识、域安全级别标识、加密算法、文件长度 (L)。对应的，若用户成功访问涉密文件，在访问后用户端会对密级标识中的最后读取者标识进行更新，更新为当前访问的用户，以便后续用户行为审计时监控。

- [0022] 用户访问密文：

[0023] 用户要访问密文时，文件系统过滤层主动提取待访问密文的密级标识与访问用户的权限比较，从而判断用户是否具有浏览该文件的权限，以便决定是否往文件系统驱动层发送 IRP 来完成涉密信息的读取与解密，当且仅当密级标识与访问用户的权限匹配时向数据文件系统驱动层发送读的 I/O 请求包的请求读取密文然后解密的步骤。

[0024] 最佳的，上述加密算法采用密钥加密，所述创建密文与访问密文中的加密、解密的密钥由服务端分发。

[0025] 如上所述，本发明利用微软内核操作系统的驱动框架，嵌入文件系统过滤层，设置在服务端的密钥管理，结合访问控制策略，构造成一个信息控制引擎，实现涉密信息的动态透明加解密与细粒度访问控制，并保证了涉密信息一旦离开该平台，将因缺失密钥管理模块而无法被明文打开。可见，信息控制引擎是整个防护系统的基础。

- [0026] 密文流通控制，包括：

[0027] 多级域信息流向控制，当密文在多级域中流通时，通过劫持密文然后根据访问策略比较密文的密级标识中的域安全级别标识是否高于当前流通域，高于则对密文执行拦截，否则对密文执行转发 / 放行的步骤；

- [0028] 同级域信息流向控制，当密文在同一级域中流通时，通过劫持密文然后根据访问

策略比较密文的密级标识中的创建者标识是否高于接收用户，高于则对密文执行拦截，否则对密文执行放行 / 转发的步骤。

[0029] 最佳的，密文流通控制在安全网关的截获下实现控制。

[0030] 由此，若是使用者通过 U 盘等外部接口，移走密文，如果是在离开该系统的机子上运行，将由于没由服务端分发的密钥而无法打开。如果是拷到别的域或者是拷到同一个域的机子，由于在解密过程中，会对域级别与信息密级标识进行判断，从而造成不符合要求的人打开失败。

[0031] 用户行为审计，包括：

[0032] 根据密文的密级标识中文件标识为身份标识进行用户行为的日志审计与危险操作下发出报警的步骤，做到责任可追查及实时监控。

[0033] 在整个过程中，用户行为审计会通过关联文件标识（ID 标识）进行跟踪，当用户发生读、写、修改、流通等操作时候，写入服务端审计数据库，对会产生信息泄露的操作进行报警。

[0034] 如图 1 为上述方法得以执行的一种系统实体架构示意图，本发明适用于 C/S 架构，通过 SSL 安全通道连接用户端与服务端，实现涉密文件的细粒度访问以及安全域管理与信息流向控制，各模块功能如下：

[0035] 利用自检扫描系统，在域管理模块进行计算机、设备的识别，绑定 IP/MAC，界面化展示整个区域网络架构、PC、服务器及相关设备，是整个域管理的基础，将划分不同安全级别的域给予形象的展示。

[0036] 用户认证模块，在用户注册时，管理员根据最小化原则，赋予某一级别权限，包括绝密、机密、秘密、敏感、公开；在用户登录时，通过页面重定向，强制用户通过 SSL 安全机制实现握手认证，建立通信安全通道。在已认证用户读取涉密信息时，就可以根据该用户权限，实现细粒度访问。

[0037] 信息控制引擎，利用 Windows 内核的驱动框架，采用改进型文件系统过滤驱动技术，在 I/O 管理器与文件驱动系统层之间嵌入文件系统过滤层，通过文件系统过滤层将密级标识附加于信息头部，并对读写过程中的驱动层之间传递的 IRP 数据包进行截获与过滤等相应操作，结合服务端的密钥管理模块，实现动态透明加解密。用户创建文件或被确认对该文件有读权限时，系统在内核层创建信息密级标识链表用来关联权限，提高读取效率。

[0038] 日志审计模块，密级标识中的文件标识（ID）作为涉密信息的唯一身份标识，系统通过关联 ID，实现对信息从生成 - 访问 - 流通 - 销毁这一系列过程进行跟踪，形成日志记录，并对用户的违规操作进行弹框报警，达到实时监控与责任追求的目的。

[0039] 密钥管理模块：内核是通过多个 IRP 读写命令来完成对文件的读写，由于每次读写信息的加解密操作都不可以改变信息长度，因此需要采用对称加密算法，而加 \ 解密所需要的密钥就是通过服务端的密钥管理模块来获取。该系统可以支持多种加密算法，用户可以根据自己的需要，在策略配置时，选择相应的加密算法。

[0040] 实施例

[0041] 上述通过认证用户创建密文，参见图 2，在一个实施例中可具体包括步骤：

[0042] A1)、通过页面重定向（是一种普通的强制认证的方式），强制用户通过 SSL 安全机制实现握手认证，建立通信安全通道，连接服务端；

[0043] A2)、用户端应用程序(用户用于打开涉密信息的应用软件,例如 word)调用操作系统读写信息函数(如 CreateFile 函数,即是 windows 框架里的读写信息时候要调用到的函数)向 I/O 管理器发送 IRP_MJ_WRITE 写请求;

[0044] A3)、I/O 管理器提取进程名称、存储路径、开始地址、数据长度、待存储数据等构造写请求对应的 I/O 请求包(IRP),并将该 IRP 发送到文件系统过滤层;

[0045] A4)、文件系统过滤驱动层收到数据包后,主动向文件系统驱动层发送一次 IRP 写请求,请求在待加密文件的文件头加入密级标识,同时在本地对应用户创建密级标识链表用于保存上述密级标识,并其更新至服务端,根据密级标识中的加密算法完成加密;

[0046] 本步骤中,由于要将正常的写过程先挂起,再由文件系统过滤驱动层完成添加密级标识的过程,所以文件系统过滤驱动层收到数据包后,需要主动的向文件系统驱动层发送一次 IRP 写请求。

[0047] A5)、文件系统过滤驱动层将添加了密级标识,并联合服务端完成的加密后的 IRP 数据包发送给文件驱动系统,并最终该带有密级标识的涉密信息以密文形式保存(例如写入物理磁盘保存)。

[0048] 而用户访问密文的实施例则参见图 3,具体包括步骤:

[0049] B1)、通过页面重定向,强制用户通过 SSL 安全机制实现握手认证,建立通信安全通道,连接服务端;

[0050] B2)、用户端应用程序调用系统内核组建提供的函数接口向 I/O 管理器发送 RP_MJ_READ 读请求;

[0051] B3)、I/O 管理器提取进程名称、存储路径、开始地址、数据长度等构造读请求对应的 IRP,并将该 IRP 发送到文件系统过滤层,等待读取返回的密文;

[0052] B4)、过滤驱动层向文件系统驱动层发送密级标识读取指令(IRP_QUERY_INFO),获取本次访问密文的密级标识;

[0053] B5)、将密级标识中的文件标识与用户的密级标识链表对比,若密级标识链表中已有,则继续步骤,若无,则进行权限的对比,若创建者标识高于接收用户权限则返回错误,否则将此密文更新到密级标识链表并同步到服务端然后继续步骤;

[0054] B6)、文件系统过滤驱动层将 IRP 发送给文件系统过滤层;

[0055] B7)、文件系统驱动层接收到数据后将本次访问密文读出并返回给文件系统过滤层;

[0056] B8)、文件系统过滤层接收到返回的密文后,按照密级标识中的加密算法解密,并将解密后的数据传给 I/O 管理器;

[0057] B9)、I/O 管理器将该数据传给用户端应用程序接口,完成读请求。

[0058] 涉密机构或企业内网,出于保密需求,都会根据自身需要划分不同级别的安全域,并根据最小化原则,赋予用户不同的角色以及对应的权限。因此,参见图 4,对于密文流通控制中,特别是多级域信息流向控制的访问策略可以进一步包括步骤:

[0059] C1)、比较密文的密级标识中的域安全级别标识与当前流通域的安全级别高低,高则执行拦截,否则继续步骤;

[0060] C2)、判断接收用户是否是拥有访问该密文的权限,是则继续步骤,否则返回错误;

[0061] C3)、对密文执行放行 / 转发。

[0062] 通过对创建者级别、域安全级别、信息秘密级别(文件标识)进行细分,辅以如上所述的访问控制策略,通过信息控制引擎与服务端,实现对涉密信息的细粒度访问,杜绝涉密信息由高密级域流向低密级域。

[0063] 本发明还提供了一种基于信息密级标识的多级域防护的系统,通过在内核操作系统的驱动框架的 I/O 管理器与文件驱动系统层之间嵌入文件系统过滤层,文件系统过滤层包括:

[0064] 通过认证用户创建密文模块,用于在收到写的 I/O 请求包请求后,向文件系统驱动层发送写的 I/O 请求包请求,从而在待加密文件中加入密级标识再通过加密算法加密后将其以密文形式保存;

[0065] 上述加密算法包括在密级标识中,密级标识还包括有创建者标识、文件标识及域安全级别标识,所述域安全级别标识与创建用户自身所在域相对应,所述创建者标识与创建用户自身的权限级别相对应;

[0066] 用户访问密文模块,包括主动提取待访问密文的密级标识与访问用户的权限比较,仅当密级标识与访问用户的权限匹配时向数据文件系统驱动层发送读的 I/O 请求包请求读取密文然后解密;

[0067] 密文流通控制模块,包括,

[0068] 多级域信息流向控制单元,用于当密文在多级域中流通时,通过劫持密文然后根据访问策略中的比较密文的密级标识中的域安全级别标识是否高于当前流通域,高于则对密文执行拦截,否则对密文执行放行 / 转发;

[0069] 同级域信息流向控制单元,用于当密文在同一级域中流通时,通过劫持密文然后根据访问策略比较密文的密级标识中的创建者标识是否高于接收用户,是则对密文执行拦截,否则对密文执行放行 / 转发;

[0070] 用户行为审计模块,用于根据密文的密级标识中文件标识为身份标识进行用户行为的日志审计与危险操作下发出报警。

[0071] 较佳的,上述通过认证用户创建密文模块具体包括:

[0072] 通信连接单元,用于通过页面重定向,强制用户通过 SSL 安全机制实现握手认证,建立通信安全通道,连接服务端然后转到写请求单元;

[0073] 写请求单元,用于当用户端应用程序调用操作系统读写信息函数向 I/O 管理器发送写请求;

[0074] 写请求反馈单元,用于当收到写请求单元的写请求后, I/O 管理器提取进程名称、存储路径、开始地址、数据长度、待存储数据等构造写请求对应的 I/O 请求包,并将该 I/O 请求包发送到文件系统过滤层;

[0075] 密文创建单元,用于文件系统过滤驱动层收到数据包后,主动向文件系统驱动层发送一次 I/O 请求包的写请求,请求在待加密文件的文件头加入密级标识,同时对应用用户创建密级标识链表用于保存上述密级标识,并将其更新至服务端,根据密级标识中的加密算法完成加密;

[0076] 密文处理单元,用于当密文创建单元完成加密后,文件系统过滤驱动层将加密后的 IRP 数据包发送给文件驱动系统,并最终该带有密级标识的涉密信息以密文形式保存。

- [0077] 较佳的，上述用户访问密文模块具体包括：
- [0078] 通信连接单元，用于通过页面重定向，强制用户通过 SSL 安全机制实现握手认证，建立通信安全通道，连接服务端然后转到读请求单元；
- [0079] 读请求单元，用于当用户端应用程序调用系统内核组建提供的函数接口向 I/O 管理器发送读请求；
- [0080] 读反馈单元，用于当收到读请求单元的读请求后吗，I/O 管理器提取进程名称、存储路径、开始地址、数据长度等构造读请求对应的 I/O 请求包，并将该 I/O 请求包发送到文件系统过滤层，等待读取返回的密文然后转至密级标识获取单元；
- [0081] 密级标识获取单元，用于过滤驱动层向文件系统驱动层发送密级标识读取指令，获取本次访问密文的密级标识；
- [0082] 密级识别单元，用于在密级标识获取单元获取密文的密级标识后，将密级标识中的文件标识与用户的密级标识链表对比，若密级标识链表中已有，则继续步骤，若无，则进行权限的对比，若创建者标识高于接收用户权限则返回错误，否则将此密文更新到密级标识链表并同步到服务端然后转到文件系统过滤层请求单元；
- [0083] 文件系统过滤层请求单元，用于文件系统过滤驱动层将 I/O 请求包发送给文件系统过滤层；
- [0084] 文件系统过滤层响应单元，用于在收到文件系统过滤层请求单元的 I/O 请求包后，文件系统驱动层将本次访问密文读出并返回给文件系统过滤层；
- [0085] I/O 管理器请求单元，用于在文件系统过滤层反馈单元返回密文后，文件系统过滤层接收到返回的密文，按照密级标识中的加密算法解密，并将解密后的数据传给 I/O 管理器；
- [0086] I/O 管理器响应单元，用于在 I/O 管理器请求单元解密密文后，由 I/O 管理器将该数据传给用户端应用程序接口，完成读请求。
- [0087] 最佳的，上述系统中各模块、单元之间锁采用的加密算法采用密钥加密，所述创建密文与访问密文中的加密、解密的密钥由服务端分发。
- [0088] 综上所述，对应背景技术所述的现有技术的 3 项不足，本发明的有益效果在于：
- [0089] 1、针对第一个缺陷，本发明采用的技术是：文件系统过滤驱动层收到数据包后，主动向文件系统驱动层发送一次 IRP 写请求，请求在文件头加入固定长度的密级标识，由于密级标识中包含有秘密级别，根据创建用户的级别默认自动赋予对应的信息密级，从而实现了信息密级细粒度划分，再根据之前描述的读与流通流程，就可以实现细粒度访问，克服背景技术里不能实现细粒度划分与细粒度访问的缺陷。
- [0090] 2、针对第二个缺陷，如前所述，由于密级标识至少中包含有三个标识，分别是密级标识、域安全级别、创建者标识。在服务端，管理员根据工作需要结合最小化原则赋予用户权限，产生创建者标识以及其所在域；企业或涉密机构根据安全级别不同进行网络区域划分，在域管理模块中通过自扫描系统实现形象化展示并用二进制标识域的安全级别；密级标识是通过文件系统过滤驱动层添加进去，里面包含文件标识、创建者标识、修改者标识、最后读取者标识，权限信息标识、域安全级别标识、加密算法、文件长度。当对文件信息进行操作，包括创建、读取、修改、流通，都会导致密级标识的更新（主要指的是密级标识中最后读取者标识），将这更新的内容同步到服务端审计数据库，就能达到信息跟踪的目的。

对比密级标识、域安全级别、创建者标识，当出现可能造成信息泄露的操作发生时候，既进行了无权限操作，将该操作通过密集标识更新到审计数据库，同时弹出报警警告。

[0091] 3、针对第三个缺陷，由于本发明实现了信息从生成－访问－流通－销毁这一系列过程的全过程跟踪标识，并记录到审计数据库中，因此在出现安全事故时候，可以导出审查，做到责任追究。

[0092] 以上所述仅为本发明的实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

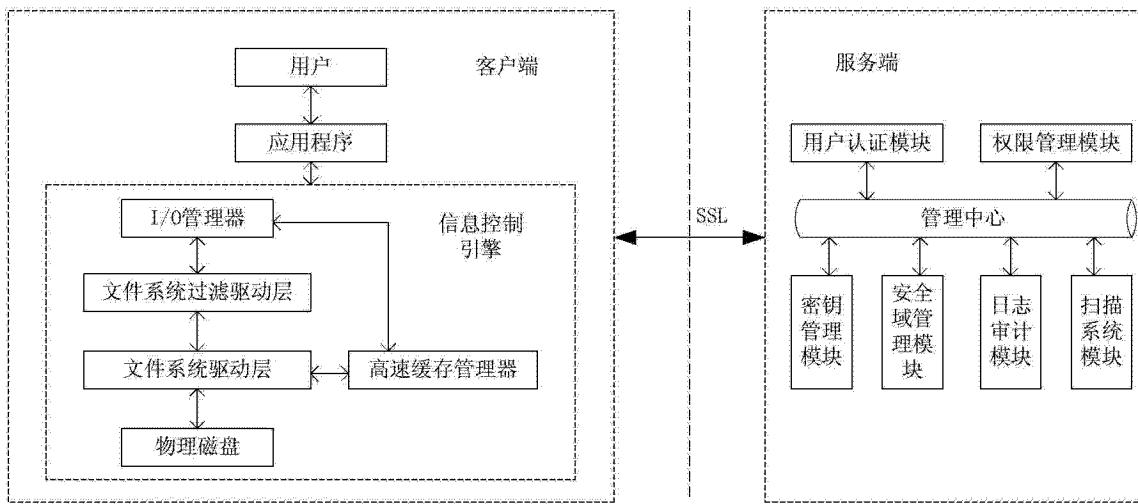


图 1

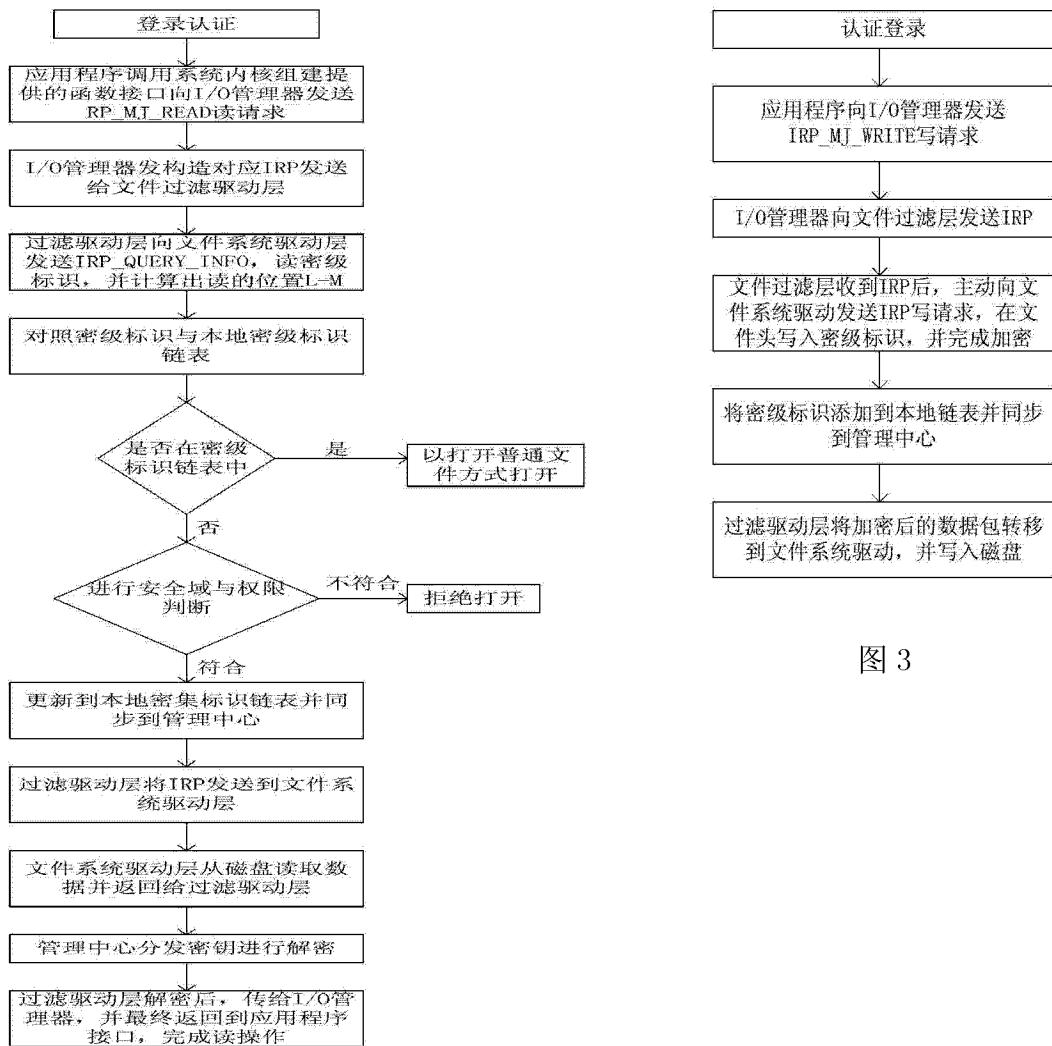


图 2

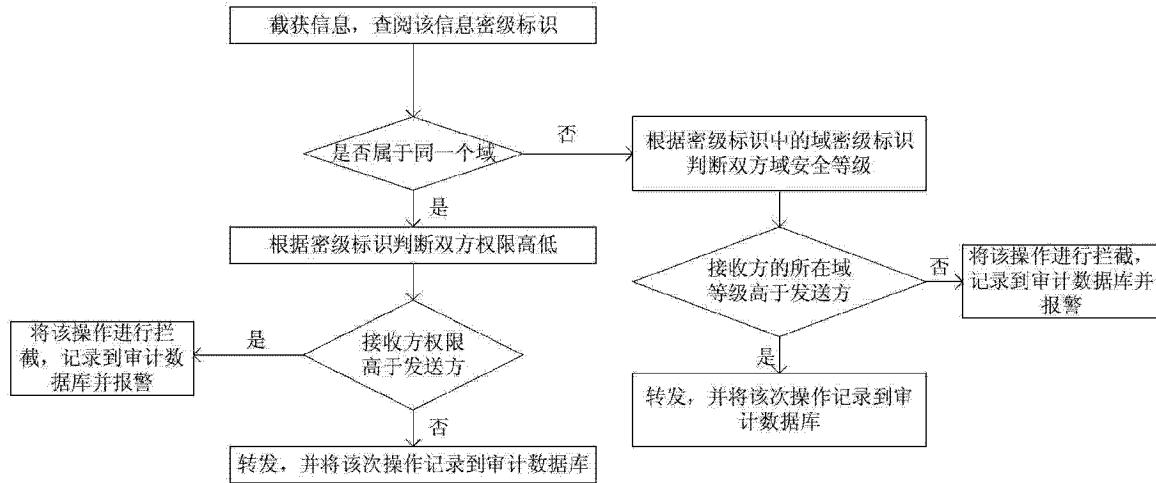


图 4