一种基于虚拟隔离机制的云盘安全访问模型

陈 锋[1] 鲍爱华[2] 张维明[1]

(国防科技大学信息系统与管理学院 长沙 410073)[1] (解放军理工大学指挥信息系统学院 南京 210007)[2]

摘 要 云盘技术是云计算领域的重要研究方向,由于存在数据泄漏方面的安全隐患,目前在持有核心数据的组织(如创新型企业、军队)中往往难以得到广泛应用。提出一种基于虚拟隔离机制的云盘安全访问模型ACIM,理论分析表明该模型能够防止企业内云盘上的敏感文件数据泄露;同时,基于该模型实现了面向企业私有云存储的电子文档集中管控系统(CFS),测试并分析了终端主机上CFS系统对文件读写操作性能的影响。目前该系统已在多个重要用户单位得到成功应用,具有广阔的应用前景。

关键词 云盘,虚拟隔离,数据安全

中图法分类号 TP393.08 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.4.024

Security Access to Cloud Disk via Virtual Isolation Mechanism

CHEN Feng[1] BAO Ai-hua[2] ZHANG Wei-ming[1]

(School of Information System and Management, National University of Defense Technology, Changsha 410073, China)[1]

(College of Command Information System, PLA University of Science and Technology, Nanjing 210007, China)[2]

Abstract The cloud storage technology is an important research area of cloud computing. Because of the hidden trouble about data leakage, cloud storage services are often difficult to be widely used in organizations with the core data, such as the innovative enterprises or the army. For this issue, a noval security access model for cloud disk was proposed via the virtual isolation mechanism. Theoretical analysis shows that the model has ability to prevent sensitive data leakage in cloud disk of the enterprise. Further, an enterprise private cloud storage-oriented electronic document centralized management and control system CFS was presented to test read/write operations performance based on the model. Until now, the system has been successfully applied to a number of important user units, and has very good development prospects.

Keywords Cloud disk, Virtual isolation, Date security

1 引言

近年来,随着云存储理念的深入发展,越来越多的企业希望搭建属于自己的云存储系统来为企业提供存储服务,国外典型的云存储服务产品有Dropbox[1]、SkyDrive[2]等,国内主要有金山[3]、奇虎360[4]等。这些云存储系统在终端用户以云盘的形式存在,提供文件自动双向同步功能,具有非常好的用户体验。对于企业单位来说,它能够对企业内部终端主机上的电子文件进行集中存储、实时同步与共享、支持移动和协同办公,具有非常大的应用前景,但也带来了极大的安全隐患:云盘中的数据文件在使用过程中存在着众多的信息泄露途径,如木马病毒窃取、用户恶意通过网络和外部设备泄露企业内部数据等等。因此,在目前开放式网络环境下,尤其是云存储环境下,如何将数据以一种可信的方式存储并保证数据在使用过程中的安全性和可靠性,已经成为计算机信息安全研究中的一个重要问题。

目前,云存储安全性相关的研究集中在数据完整性、访问控制和数据加密等几个方面。针对云存储数据完整性问题,曹夕等人提出了一种云存储系统中数据完整性验证协议CS-DIV[5],在考虑系统资源和带宽的情况下适应性地随机验证数据块确认完整性;颜湘涛等人[6]提出了一种基于哈希树的云存储完整性检测算法,利用哈希树结构和大数模运算进行数据完整性检测。在访问控制和数据加密方面,刘帆[7]提出了一种用于云存储的CP-ABE方案,以防止云存储特权用户的内部攻击。对于整个云盘系统,上述研究主要关注于云存储服务器端的数据安全性,忽视了云盘中数据在使用过程中传输到终端主机上的安全性。

对于数据在终端主机上的防泄露问题,部分研究者将一部分数据处理和安全控制功能集成到存储设备中以增强存储设备的安全性,提出了主动存储[8]、自安全磁盘[9]等方法。靳超等[10]重点基于面向对象方法实现主动存储;赵跃龙[11]等则研究了以虚拟存储映射方式实现的网络智能磁盘。这些研究主要侧重提高数据存储的安全性,而较少考虑计算机终端的应用环境和进程对数据的使用是否可信。为此,VMware[12]等厂商提出了虚拟桌面架构,通过虚拟隔离改善了软件运行环境的可信性。King[13]等人提出了利用虚拟机监视

到稿日期:2015-02-05 返修日期:2015-07-20 本文受国家自然科学基金项目(912024006)资助。

陈 锋(1979-),男,博士,讲师,主要研究方向为网络与信息安全、密码学,E-mail:chenfeng@nudt.edu.cn;鲍爱华(1981-),男,博士,讲师,主要研究方向为云计算、语义Web服务;张维明(1963-),男,博士,教授,博士生导师,主要研究方向为信息安全、信息决策。

器为用户程序提供安全保护层，隔离保护用户程序的内存空间，确保软件运行环境可靠。虚拟化技术促进了软件运行环境的可信性研究。Bussani[14]提出了可信虚拟域，它能够为敏感数据应用环境提供可信性保障。Gasmi[15]等人提出一种基于可信虚拟域的安全可扩展的企业版权管理方案，它通过虚拟机机制建立可以满足隔离特性的可信执行环境。这些基于硬件层虚拟机的实现比较适合于分布式服务器应用中的数据保护，而对于终端存储中的数据保护，这种方式开销较大。Yang Yu[16]设计实现了一种轻量级的虚拟机 FVM，通过系统调用的监控和重定向，为进程提供一个隔离的运行环境，通过对进程的写操作进行限制，防止对系统资源完整性造成的破坏，具有较好的可用性，但没有考虑机密性保护的需求。

总之，目前在云环境下的数据保护方面，已有的模型要么聚焦于云存储服务器本身，将相关的保护技术叠加在云端存储设备或者存储系统上，较少考虑访问数据的端用户，无法确保数据到达用户端后的安全性；要么基于硬件层虚拟机实现用户数据和运行环境的隔离，对端用户资源要求高，性能无法满足需求，且割裂了用户熟悉的环境和使用习惯。本文提出一种基于虚拟隔离机制的云盘安全访问模型 ACIM（Access to Cloud Disk via Virtual Isolation Mechanism），理论分析表明该模型解决了云环境下关键数据在端用户处可能存在的信息泄露问题，保证了云盘系统用户端的安全性；同时，该模型对端用户资源要求不高，对客户端系统的性能和用户的使用习惯影响较小，方便在实际中部署和使用。在实践中基于该模型实现了面向企业私有云存储的电子文档集中管控系统（CFS），测试并分析了终端主机上 CFS 系统对文件读写操作性能的影响。目前该系统已成功应用于多个重要用户单位，具有广阔的应用前景。

2 ACIM 模型

企业内各终端主机上的电子文件一般与企业自身核心业务紧密关联，在使用过程中面临各种安全风险。本文对文件数据所有权做如下假设。

假设 1　企业内所有文件数据归企业自身所有，即云盘和云存储服务器内所有文件数据的所有权主体是企业；企业成员个体对文件数据具有使用权限，但不具有所有权。

根据该假设，企业文件数据在使用过程中面临两类威胁主体：内部威胁即企业内部成员，他们可能会有意无意地泄露以及通过网络和外部设备泄露；外部威胁，即网络黑客、木马等。

此外，云盘系统的运行环境比较复杂，涉及网络、服务器等各种安全风险，在本文中为了简化问题，提出如下假设。

假设 2　云盘在主机上以文件夹的方式存在，该文件夹内所有文件数据是企业成员所在云存储服务器账号内文件数据的镜像。

假设 3　云盘文件数据与企业成员对应云存储服务器账号内文件数据保持双向实时同步，即任何文件数据在云盘或云存储服务器内的改变都会立即同步到对方，使文件数据在云盘和云存储服务器内是一致的。

假设 4　云盘内文件数据以密文存储，对应的云存储服务器内文件数据也以密文存储，使用安全可靠的密钥管理系统。云盘与云存储服务器之间的通信是安全可靠的；云存储服务器上的文件数据是安全可靠的。

定义 1　经安全检测无恶意代码的进程，本文称之为可信进程，否则称之为非可信进程。

定义 2　若该进程对内存的访问、对磁盘的读写操作、对网络及计算机外部设备（如打印机）等的访问操作受安全机制实时监控，则称之为受控进程。

基于上述假设，本文提出了云盘文件虚拟化隔离安全访问模型。它的主要思想：把终端主机上的进程分为可信进程和非可信进程两类；云盘文件以密文方式存储，所有进程对它的访问操作都须经过“I/O 代理进程”转发，“I/O 代理进程”以透明写加密/读解密的方式对云盘文件进行读写操作；非可信进程禁止访问云盘文件，可信进程一旦访问云盘文件，它的状态转变为受控进程，被强制置于虚拟隔离运行环境中运行；在该环境下，受控进程对数据的访问处于安全隔离状态，以保证数据不外泄。

图 1 是云盘文件虚拟化隔离访问模型，图中有向箭头表示数据的流向。

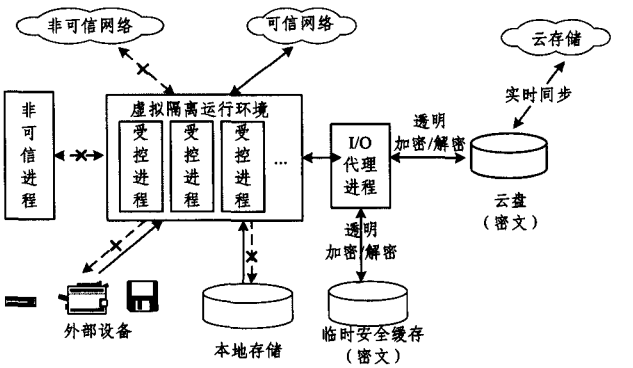

图 1　云盘文件虚拟化隔离访问模型

该模型主要由 3 部分构成。

（1）安全云盘。它以网络硬盘形式展现，云盘内的文件通过数据加密方式安全存储在本地，同时通过实时双向文件同步技术，以加密安全传输的方式与云存储服务器保持同步，副本以密文存储在云端。

（2）虚拟隔离运行环境（Virtual Isolated Execution Environment，VIEE）。当进程尝试读取云盘内的文件时，该进程将标记为受控进程，被强制置于在该环境下进行隔离运行。隔离包括以下 5 个方面：

①受控进程运行时的内存数据被隔离保护，无法与非可信进程进行交互；

②受控进程对云盘文件的读写操作，全部由 I/O 代理进程进行安全控制；

③受控进程以只读方式使用本地磁盘数据，对本地存储的所有文件的写操作都通过 I/O 代理进程以重定向方式，加密写入临时安全缓存进行隔离，读取时通过代理程序解密读取；

④受控进程只能以只读方式使用本地外设，如 U 盘、打印机等写操作被禁止；

⑤受控进程只能访问指定的可信网络，隔离其对风险网络的访问。

（3）I/O 代理进程。系统内所有进程对云盘和临时安全缓存内文件的访问都需要经过该代理程序，由该程序根据策略对其操作进行控制，若该进程为可信进程，则对云盘内文件

进行透明读写操作，并把结果数据安全转发给访问进程；非可信进程禁止访问云盘和临时安全缓存。

通过上述云盘文件虚拟化隔离访问安全机制，用户登录云盘后就如同进入“银行金库”来使用其自身数据，非可信进程无法入侵，只有受控进程可以访问，敏感数据加密存储，且在隔离运行环境下安全使用，防止被泄漏。

3 VIEE 实现

隔离控制的核心是程序运行环境，本质上可以看作是将数据与程序一起划为安全域。而实际上访问云盘文件的受控进程运行时，它须访问相关配置文件和临时文件（这些文件由于是进程运行必需的，因此被称为进程运行文件，简称运行文件），这些文件一般在云盘外，对于这种可能跨越安全域和非安全域的进程，单纯的隔离虽然可以保证数据的安全性，但是会破坏进程运行环境导致进程运行错误。

本文在 windows 平台下设计并实现了一个虚拟隔离运行环境（VIEE）。图 2 示出隔离虚拟运行环境模型，它把可信网络、临时安全存储、云盘和受控进程划为一个安全域。在该环境内，利用网络访问过滤技术，受控进程只允许访问可信网络；利用内存空间保护技术，受控进程的运行内存空间被监控保护，防止非法进程跨进程读取敏感数据；利用文件过滤驱动技术，受控进程访问运行文件被单向隔离控制。这样通过综合运用 3 种技术构成虚拟隔离运行环境，使数据只会流动于安全域内，防止敏感数据外泄。

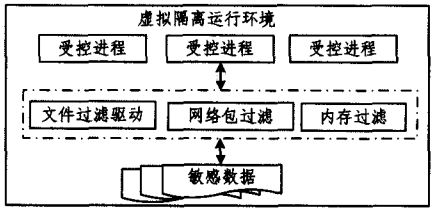

图 2 虚拟隔离运行环境模型

基于网络包过滤技术，受控进程根据访问控制列表 ACL 对受控进程的网络访问进行数据包过滤，使它只能与可信网络进行安全通信；同时为了保证数据的安全性，要求可信网络内所有进程都处于隔离虚拟运行环境内执行。

基于内存空间保护技术，利用 API HOOK 监控受控进程对剪贴板和跨进程的读写操作，禁止非可信进程访问剪贴板内的敏感数据，允许可信进程访问剪贴板内的敏感数据，但是它一旦访问，该进程就会被标注为受控进程，被强制置于 VIEE 下进行隔离运行。同时利用 API HOOK 监控对注册表的访问操作，将对注册表的写操作重定向到虚拟注册表内，禁止非可信进程访问虚拟注册表内的敏感数据，允许可信进程访问虚拟注册表，但是它一旦访问，该进程也会被标注为受控进程，被强制置于 VIEE 下进行隔离运行。

基于文件过滤驱动技术，受控进程对非云盘内文件进行写操作时，将会触发动态重定向操作：若是创建或写运行文件请求，则在临时安全缓存中拷贝产生对应的副本文件，再将该请求重定向到临时安全缓存中进行访问；如果是其它访问请求，如读请求，则将请求重定向到对应的副本文件，对该副本进行操作。通过重定向操作，可以确保受控进程可以任意读取 U 盘等外设内文件数据以及本地存储上运行的文件数据，但是在使用过程中这些数据只会流动于安全域内。为不影响上层应用程序的执行，重定向操作需要在应用层以下实现并且对上层应用透明，本文采取开源 dokan[17] 开发库进行实现。

图 3 是基于 dokan 的文件系统框架，其中 dokan. sys 是内核态文件系统驱动，创建文件系统（实现 Dokan 库的 API）的程序被称为文件系统程序。用户程序提出的文件操作请求（例如 CreateFile、ReadFile、WriteFile）会送到 Windows I/O subsystem（内核中运行），后者会继续将请求送到 dokan. sys。文件系统程序利用 dokan. dll 提供的函数将回调函数注册到 dokan. sys 中，后者会在收到请求之后调用这些函数。回调函数的结果会送回到提出请求的程序。该框架中的 dokan. sys 相当于一个运行在内核态的代理，作为提出请求的程序和实现各种操作的文件系统程序的桥梁。

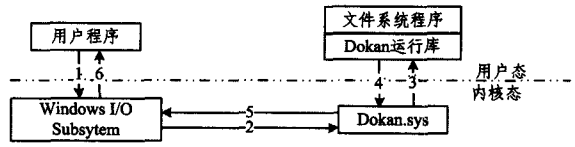

图 3 基于 dokan 的文件系统框架

在实现过程中实现 CreateFile、ReadFile、WriteFile 等 21 个回调函数，其中核心函数 WriteFile 算法如表 1 所列，ReadFile 算法如表 2 所列。

表 1 WriteFile 算法

算法输入：进程 p，文件 f_i，数据 d
算法输出：修改后文件 f_o
MirrorWriteFile()
1. 若 p 是受控进程
1.1 采取加密算法 RC4 对数据 d 加密，即 d_1 = Encrypt(d)
1.2 若文件 f_i 属于云盘内文件，则直接写入 f_o = WriteFile(f_i, d_1)
1.3 若文件 f_i 不属于云盘内文件
1.3.1 若临时安全缓存内不存在对应文件，则读取整个文件数据，对该文件加密 f' = RC4(f_i)，再写入临时缓存 f_o = WriteFile(f', d_1)
1.3.2 若临时安全缓存内存在对应文件，写入临时缓存 f_o = WriteFile(f_i, d_1)
2. 若 p 是非受控进程
直接写入 f_o = WriteFile(f_i, d)

表 2 ReadFile 算法

算法输入：进程 p，文件 f_i，数据起始位置 pos，数据大小 size
算法输出：数据 d，进程状态 S_p
MirrorReadFile()
1. 若 f_i 不属于云盘文件
1.1 读取文件数据 d = ReadFile(f_i, pos, size)
1.2 进程状态 S_p 保持不变
2. 若 f_i 属于云盘文件
2.1 令 f' 为 f_i 在安全缓存内对应的加密文件
2.2 读取 f' 内对应位置数据 d' = ReadFile(f', pos, size)
2.3 解密 d = Decrypt(d')，修改进程状态 S_p 为受控进程

4 性能测试与分析

基于 ACIM 模型，实现了面向企业私有云存储的电子文档集中管控系统（CFS）。该系统既支持对企业内敏感数据文件进行集中存储，又能够保证终端用户通过网络访问敏感数据文件不泄露。为了测试终端主机上 CFS 系统对文件读写性能的影响，本文在如下环境下进行了两项性能测试。硬件平台：Intel（R） Core（TM）2 Duo CPU 2. 4GHz，2. 39GHz，RAM 为 1. 94GB，硬盘为 300GB，转速 7200rpm，缓存 64MB。操作系统：Windows XP SP3。

(1)相同文件的读写性能影响测试

由于操作系统对文件的读写具有缓存机制，每次读、写操作数据块的大小会影响整个文件的性能，为了排除该因素的影响，本文对每个文件全文读写时都采取 1kB 字节数据块为单位缓存。图 4 是实验结果，其中横坐标表示每次实验的文件大小，纵坐标表示 CFS 系统对文件读写操作性能的损耗百分比。从图中可知，随着文件大小增大，CFS 系统对读写性能的损耗逐步加大，这是因为在 dokan 开发库下，每次读写操作都要将请求传送到应用层做加解密(CFS 系统采取 RC4 加密算法)等计算处理，然后再发向驱动层，这需要比较大的计算开销。同时，对于相同大小的文件，读操作的性能损耗相对写操作高，原因是 CFS 系统每次读操作引发的驱动与应用层的交互以及加解密等计算开销远大于原系统的直接读操作时间开销。

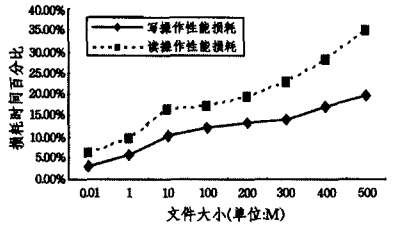

图 4　相同文件的读写性能影响

(2)应用软件的性能影响测试

在 CFS 系统中，状态为受控进程的应用软件，可能会并发地对大量的不同文件进行读写访问操作。为了测试 CFS 系统对其性能的综合影响，本文选择了常用的 5 款软件，通过其对不同大小类型文件(其中，notepad 的类型文件为 txt，winword 为 doc，excel 为 xls，autoCAD 为 dwg，photoshp 为 psd)的读、写操作来测试其性能，表 3 为实验结果。从表中可知，随着文件大小增大，CFS 系统对读写性能的损耗逐步加大，并且各种软件性能损耗不同，原因在于 3 方面。首先是每次读写操作都要将请求传送到应用层做加解密(CFS 系统采取 RC4 加密算法)等计算处理，然后再发向驱动层，这需要比较大的计算开销；其次，软件对类型文件进行处理时，需要读取本地存储上的运行文件，在对运行文件进行写操作时，在临时安全缓存中创建该文件的副本，并将写操作请求重定向到对该副本的操作，这会产生新增的时间开销，例如，WinWord.exe 对 doc 类型文件写操作时，需要从 WinWord.exe 的安装目录下读取各种配置文件，此时它需要先把这些配置文件拷贝到临时安全存储中，然后再向该副本进行写操作；最后，各种软件性能损耗不同的原因在于不同的软件其文件读写的缓存大小不同，读写类型文件(如 doc、xls 等)引发的访问运行文件大小和数目不同。

表 3　应用软件的性能影响

文件大小/M	winword	excel	autoCAD	notepad	photoshop
0.01	1.50%	1.40%	3.50%	1.30%	2.50%
1	7.50%	7.90%	12.50%	6.50%	9.50%
10	10.20%	11.00%	14.20%	7.20%	12.20%
100	16%	15%	19%	12%	18%
200	17%	18%	24%	13%	19%
300	18%	19%	26%	15%	22%
400	18%	20%	30%	16%	24%
500	19%	22%	38%	17%	27%

5　安全性分析

ACIM 模型的安全性在于防止云盘内的文件数据在存储、读写过程中发生泄漏。为了分析该特性，本文基于 Denning[18] 的信息流模型对 ACIM 模型中的信息流进行描述和分析，将安全控制规则转换为信息流规则，进一步给出 ACIM 的数据防泄漏安全定理。

令 DS、DC 和 DL 分别表示主机上云盘内的文件集合、临时安全缓存内文件集合和其它本地文件集合；$f_1, f_2, \cdots, f_n \in (DS \cup DC \cup DL)$，$n \in \mathrm{N}$，表示主机中的文件；$PC$、$PT$ 和 PD 分别表示虚拟隔离运行环境 VIEE 内的受控进程、VIEE 外的可信进程集合和非可信进程；$p_1, p_2, \cdots, p_m \in (PC \cup PT \cup PD)$，$m \in \mathrm{N}$，表示主机上系统运行的进程；$\rightarrow_t$ 表示 t 时刻的信息流请求；$\rightarrow_t$ 表示 t 时刻的实际信息流动。根据 ACIM 的进程读写文件数据的控制机制，给出如下信息流规则。

规则 1　若可信进程和非可信进程请求读云盘内的文件和临时安全缓存内的文件，被拒绝访问，即

$$\forall f \in_{t_0} (DS \cup DC), p \in_{t_0} (PT \cup PD), f: \rightarrow_{t_0} p \Rightarrow \forall t > t_0, f \in_t (DS \cup DC)$$

规则 2　若虚拟隔离运行环境 VIEE 外的可信进程请求读云盘中的文件，在规则允许的情况下，将该进程放置到 VIEE 内受控运行，该进程转变为受控进程，即

$$\forall f \in_{t_0} DS, p \in_{t_0} PT, f: \rightarrow_{t_0} p \Rightarrow f \rightarrow_{t_0} p \wedge \forall t > t_0, p \in_t PC$$

规则 3　若虚拟隔离运行环境 VIEE 内的受控进程请求对云盘外的文件进行写操作，则在临时安全缓存中创建该文件的副本，并将写操作请求重定向到对该副本的操作，即

$$\forall f \in_{t_0} DL, p \in_{t_0} PC, p: \rightarrow_{t_0} f \Rightarrow CreateAndCopy(f', f) \wedge (p \rightarrow_{t_0} f' \wedge t > t_0, f' \in_t DC)$$

规则 4　若虚拟隔离运行环境 VIEE 内的受控进程与 VIEE 外的进程进行数据交互通信，在规则允许的情况下，需要将 VIEE 外的进程放置到 VIEE 内受控运行，该进程转变为受控进程，即

$$\forall p \in_{t_0} PT \cup PD, p' \in_{t_0} PC, p: \rightarrow_{t_0} p' \Rightarrow p \rightarrow_{t_0} p' \wedge \forall t > t_0, p' \in_t PC$$

基于以上规则，可得到在 ACIM 模型下数据防泄漏的安全定理。

定理 1　在 ACIM 模型下，云盘内文件内容在访问和使用过程中不会泄露到云盘和临时安全缓存外。

证明：采取反证法证明。假设云盘内文件内容可以泄露到云盘和临时安全缓存外，即存在如下信息流：

$$\exists f \in_{t_0} DS, \exists t > t_0, f' \in_t DL, f \rightarrow_t f'$$

由于信息具有传递性，且信息流动主要由进程对文件的读、写以及进程间通信 3 种操作触发，因此有：

$$\exists p \in_{t'} (PC \cup PT \cup PD), t_0 < t' < t'' < t, f \rightarrow_{t'} p, p \rightarrow_{t''} f'$$

由规则 3 可知，由于受控进程禁止写文件数据到本地文件集合中，因此 $p \in_{t'} PT \cup PD$，否则不存在 $p \rightarrow_{t''} f'$。

下面对 $p \rightarrow_{t''} f'$ 存在的 2 种情况进行讨论分析：

(1)若 p 在 t' 时刻直接读取 f，若根据规则 1，p 会被拒绝读取；若根据规则 2，$p \in_{t'} PS$，与 $p \in_{t'} (PT \cup PD)$ 矛盾。

(2)$\exists p' \in_{t'} (PC \cup PT \cup PD), t_0 < t''' < t', f \rightarrow_{t'} p' \wedge p' \rightarrow_{t'} p$。

(下转第 154 页)

velope Detection Based on Sliding Window ICA and Its Application to Brain-Computer Interface[J]. Acta Biophysica Sinica, 2012,28(11):896-909(in Chinese)
吴小培,宋俊可,郭晓静,等. 基于滑动窗独立分量分析的在线包络检测新方法及其在脑-机接口中的应用[J]. 生物物理学报, 2012,28(11):896-909

[10] Oppenheim A V, Willsky A S, Nawab S H. Signals and systems [M]. Englewood Cliffs, NJ: Prentice-Hall, 1983

[11] Yang Yue-xiang. The Research on the Algorithms of Information Hiding and Network Traffic Detection Based on Wavelet Analysis[D]. Changsha: National University of Defense Technology, 2008(in Chinese)
杨岳湘. 基于小波变换的信息隐藏与网络流量检测方法研究[D]. 长沙:国防科学技术大学,2008

[12] Yang Ji-peng, Liu Xue-cheng. Study of The NetWork Abnormal Detection Based on The Wavelet Transforms[J]. Journal of Shanghai Agicultural University(Natural Science), 2011(1):95-99(in Chinese)
杨继鹏,刘学诚. 基于小波变换的网络异常检测研究[J]. 山东农业大学学报(自然科学版),2011(1):95-99

(上接第 121 页)

由规则 4 可知,$p' \in_{t'} (PT \cup PD)$,因为受控进程的状态不可能转换为非可信进程和可信进程,与 $p \rightarrow_{t'} f'$ 类似递归分析 $p \rightarrow_{t'} f'$,必然存在 p^0 在 t_0 时刻直接读取 f,且 $p^0 \in_{t_0} (PT \cup PD)$,由(1)知,也存在矛盾。

综上所述,假设 $\exists f \in_{t_0} DS$, $\exists t > t_0$, $f' \in_t DL$, $f \rightarrow_t f'$ 不合理,故结论成立。

根据定理 1 可知,云盘内文件内容在访问和使用过程中将被限制于云盘和临时安全缓存内;由于云盘和临时安全缓存内的文件数据是加密存储,且只能由受控进程访问,因此外部威胁主体(如木马、病毒)进程无法解密访问,而内部威胁主体即企业内部成员,虽然通过受控进程可以解密访问,但是无法携带明文数据离开该主机和云盘系统(除非在信息安全管理员授权许可的情况下),避免泄密事件发生。

结束语 根据云盘的安全需求,本文提出了一种基于虚拟隔离机制的云盘安全访问模型。该模型主要由安全云盘、虚拟隔离运行环境和 I/O 代理进程组成,能够有效保证数据的受控访问并防止泄漏。其中,虚拟隔离运行环境 VIEE 是该模型的核心,本文重点描述了 VIEE 的设计与实现。VIEE 把可信网络、临时安全存储、云盘和受控进程划为一个安全域,利用网络访问过滤技术、内存空间保护技术和文件过滤驱动技术构建虚拟隔离运行环境,使数据只会流动于安全域内,从而防止敏感数据外泄。随后,基于虚拟隔离机制的云盘安全访问模型,本文实现了原型系统(CFS),测试并分析了终端主机上 CFS 系统对文件读写操作性能的影响。最后,通过安全性分析,证明了基于虚拟隔离机制的云盘安全访问模型的数据安全性。

在下一步研究中,将进一步测试该模型对各种应用软件的性能影响,分析性能影响由哪些因素导致,从而提出算法优化方案。

参 考 文 献

[1] https://www.dropbox.com

[2] https://skydrive.live.com

[3] http://www.ksyun.com

[4] http://yunpan.360.cn

[5] Cao Xi, Xu Li, Chen Lan-xiang. Data integrity verification protocol in cloud storage system[J]. Journal of Computer Applications, 2012,32(1):8-12(in Chinese)
曹夕,许力,陈兰香. 云存储系统中数据完整性验证协议[J]. 计算机应用,2012,32(1):8-12

[6] Yan Xiang-tao, Li Yi-fa. Integrity Checking Algorithm Based on Hash Tree for Cloud Storage[J]. Computer Science, 2012, 39(12):94-97(in Chinese)
颜湘涛,李益发. 基于哈希树的云存储完整性检测算法[J]. 计算机科学,2012,39(12):94-97

[7] Liu Fan, Yang Ming. Ciphertext policy attribute based on encryption scheme for cloud storage[J]. Application Research of Computers, 2012,29(4):1452-1456(in Chinese)
刘帆,杨明. 一种用于云存储的密文策略属性基加密方案[J]. 计算机应用研究,2012,29(4):1452-1456

[8] Lim H, Kapoor V, Wighe C. Active disk file system: Adistributed, scalable filesystem[C]// Proceedeths of the Eighteenth IEEE Symposium. Washington, DC: IEEE Computer Society, 2001:101-114

[9] Swank J D, Goodson G R, Scheinholtz M L, et al. Self-securing storage: Protecting data incompromised systems[C]// Proc of the 4th Symposium on Operating Systems Design and Implementation. Berkeley, CA: USENIX Association, 2000:12-26

[10] Jin Chao, Zhen Wei-min, Zhang You-hui. Active Storage Architecture[J]. Chinese Journal of Computers, 2005, 28(6): 1013-1020(in Chinese)
靳超,郑纬民,张悠慧. 主动存储系统结构[J]. 计算机学报, 2005,28(6):1013-1020

[11] Zhao Yue-long, Jiang Qian. Research and Design of the Virtualization Storage Technology Based on Intelligent Network Disk [J]. Journal of Computer Research and Development, 2009, 46(Suppl):44-49(in Chinese)
赵跃龙,蒋骞. 基于智能网络磁盘的虚拟存储技术的研究与设计[J]. 计算机研究与发展,2009,46(Suppl):44-49

[12] Using virtual desktop to improve the ability of the management and control [EB/OL]. [2010-3-15]. http://www.vmware.com/cn/solutions/desktop

[13] King S T, Dunlap G W, Chen P M. Operaring System Support for Virtual Machines[C]// Proc of the 2003 Annual USENIX Technical Conference. 2003:6

[14] Griffin J L, Jaeger T, Perez R, et al. Trusted virtual domains: Toward secure distributed services[C]// Proceedings of the 1st IEEE Workshop on Hot Topics in System Dependability. Los Alamitos: IEEE Computer Society. 2005:274-281

[15] Gasmi Y, Sadeghi A-R, Stewin P, et al. Flexible and Secure Enterprise Rights Management Based on Trusted Virtual Domains [C]// Proc of the 3rd ACM Workshop on Scalable Trusted Computing. 2008:71-88

[16] Yang Yu. OS level virtualization and its applications [D]. New York: Stony Brook University, 2007

[17] http://dokan-dev.net/en

[18] Denning D E. A lattice model of secure information flow[J]. Communications of the ACM, 1976, 19(5):236-243