(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 101452397 B
(45)授权公告日 2012.08.22

(21)申请号 200810203451.X
(22)申请日 2008.11.27
(73)专利权人 上海交通大学
地址 200240 上海市闵行区东川路 800 号
(72)发明人 翁楚良 王观海 骆源 李明禄
(74)专利代理机构 上海汉声知识产权代理有限公司 31236
代理人 郭国中
(51)Int.Cl.
G06F 9/455(2006.01)

(56)对比文件
CN 101290586 A,2008.10.22,
WO 2007130386 A2,2007.11.15,
CN 101305333 A,2008.11.12,
CN 1918549 A,2007.02.21,

审查员 郭全萍

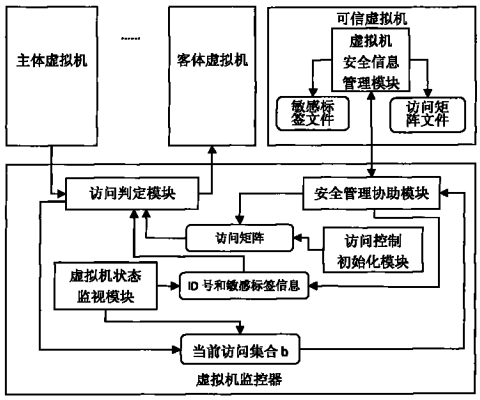
权利要求书 4 页 说明书 11 页 附图 3 页

(54)发明名称

虚拟化环境中的强制访问控制方法及装置

(57)摘要

一种计算机应用技术领域的虚拟化环境中的强制访问控制方法及装置，本发明方法在虚拟化环境中指定一个虚拟机作为具有安全管理权限的可信虚拟机，可信虚拟机使用（安全密级、安全范畴）作为敏感标签标识单个虚拟机的安全级别，建立访问矩阵设置每个虚拟机对其他虚拟机的访问类型集合；当某个虚拟机主体以某种类型访问某个虚拟机客体的，根据主客体双方的敏感标签和访问矩阵中主体对客体的访问类型集合判定这次访问是否允许。本发明装置包括访问控制初始化模块、虚拟机状态监视模块、访问判定模块、安全管理协助模块和可信虚拟机中的虚拟机安全信息管理模块。本发明可以在多级安全的虚拟化环境中有效的控制虚拟机之间的通信和资源共享。



CN 101452397 B

1. 一种虚拟化环境中的强制访问控制方法，其特征在于，包括如下步骤：

步骤一，在虚拟化场景中指定一个虚拟机作为具有安全管理权限的可信虚拟机，并以这个可信虚拟机为根，其他虚拟机为可信虚拟机的子节点建立层次关系，除可信虚拟机之外的其他所有虚拟机处于同等的地位；

步骤二，可信虚拟机使用敏感标签对其他单个虚拟机安全级别进行标识，所述敏感标签包括安全密级和安全范畴；

步骤三，可信虚拟机建立访问矩阵文件，访问矩阵文件中记录每个包含可信虚拟机在内的虚拟机对其他虚拟机的访问类型集合，访问类型包括：只读、只写和读写三种，访问矩阵中的数据在虚拟机监控器启动时被加载到虚拟机监控器内部；

步骤四，当一个虚拟机启动时，把它的 ID 号、敏感标签作为参数传入虚拟机监控器内部，在虚拟机监控器内部记录这些信息，并为该虚拟机建立一个当前访问集合 b，记录该虚拟机作为主体时当前的、所有的、以某种类型对作为客体的虚拟机的访问信息，当前访问集合 b 包含访问类型集合；

步骤五，当通信或资源共享行为发生时，检查作为主体的虚拟机和作为客体的虚拟机的敏感标签和访问矩阵是否满足敏感标签安全特性和访问矩阵安全特性，如果满足则允许作为主体的虚拟机访问客体，否则不允许作为主体的虚拟机访问客体并返回出错消息；

所述敏感标签安全特性，是指：当作为主体的虚拟机对作为客体的虚拟机进行只读访问时，作为主体的虚拟机的敏感标签必须支配作为客体的虚拟机的敏感标签；当作为主体的虚拟机对作为客体的虚拟机进行只写访问时，作为主体的虚拟机的敏感标签必须被作为客体的虚拟机的敏感标签支配；当作为主体的虚拟机对作为客体的虚拟机进行读写访问时，作为主体的虚拟机的敏感标签必须等于作为客体的虚拟机的敏感标签；

所述访问矩阵安全特性，是指当作为主体的虚拟机对作为客体的虚拟机进行只读、只写或者读写类型的访问时，其访问类型存在于访问矩阵中代表作为主体的虚拟机对作为客体的虚拟机的访问类型集合中；

步骤六，当步骤五返回的结果是允许访问时，在作为主体的虚拟机的当前访问集合 b 中加入一条这次访问的记录；

步骤七，当作为主体的虚拟机结束对作为客体的虚拟机的一次访问时，从当前访问集合 b 中删除关于这次访问的记录；

除可信虚拟机以外的虚拟机的敏感标签，其中的安全密级采用数值形式，安全范畴为特定访问权限的集合，集合中的每个元素代表一项特定的访问权限，两个敏感标签之间的关系是支配与被支配、等于或者不可比较的关系；

所述对单个虚拟机的安全级别进行标识，具体如下：如果被标识的虚拟机没有敏感标签，则直接使用敏感标签标识该虚拟机的安全级别；如果被标识的虚拟机已经具有敏感标签，则使用新敏感标签重新标识该虚拟机的安全级别，即调整该虚拟机的安全级别，如果标识安全级别时，虚拟机正在运行则需要所有正在运行的虚拟机的当前访问集合 b 同时满足下述 6 个当前访问集合 b 的安全特性，标识操作才能成功：

①被标识的虚拟机的新敏感标签能够支配所有其他正在运行的虚拟机的当前访问集合 b 中对被标识的虚拟机进行只写访问的虚拟机的敏感标签；

②所有其他正在运行的虚拟机的当前访问集合 b 中对被标识的虚拟机进行只读访问

的虚拟机的敏感标签能够支配所有其他正在运行的虚拟机的新敏感标签；

③所有其他正在运行的虚拟机的当前访问集合 b 中对被标识的虚拟机进行读写访问的虚拟机的敏感标签等于该虚拟机的新敏感标签；

④被标识的虚拟机的新敏感标签必须支配它自己的当前访问集合 b 中所有被该虚拟机只读访问的其他虚拟机的敏感标签；

⑤被标识的虚拟机自己的当前访问集合 b 中所有被它只写访问的其他虚拟机的敏感标签能够支配该虚拟机的新敏感标签；

⑥被标识的虚拟机的新敏感标签等于它自己的当前访问集合 b 中所有被该虚拟机读写访问的其他虚拟机的敏感标签；

所述每个虚拟机对其他虚拟机的访问类型集合，其中不能设置其他虚拟机对可信虚拟机的访问类型集合，即所有其他虚拟机不能作为主体与可信虚拟机通信，可信虚拟机不能作为客体出现在通信过程中；

所述通信或资源共享行为发生时，如果在通信过程中作为主体的虚拟机是可信虚拟机，则不受敏感标签安全特性和访问矩阵安全特性两个条件的约束，即可信虚拟机能够以任意类型访问其他虚拟机。

2. 一种根据权利要求 1 所述方法的虚拟化环境中的强制访问控制装置，其特征在于，包括：虚拟机安全信息管理模块、访问控制初始化模块、虚拟机状态监视模块、访问判定模块、安全管理协助模块，其中，

虚拟机安全信息管理模块设置在可信虚拟机中，将其他虚拟机作为可信虚拟机的子节点，建立起虚拟机的层次关系，同时，使用敏感标签标识其他虚拟机的安全级别，在访问矩阵中设置每个虚拟机对其他虚拟机的访问类型集合，并将上述操作结果一方面保存到可信虚拟机的磁盘文件中，另一方面输出到虚拟机监控器内部；

访问控制初始化模块设置在虚拟机监控器内部，访问控制初始化模块在虚拟机监控器启动的过程中，从可信虚拟机的磁盘中把访问矩阵加载到虚拟机监控器的内部，在虚拟机启动与关闭、虚拟机之间通信和资源共享的关键路径上设置安全钩子函数，供虚拟机状态监视模块和访问判定模块使用；

虚拟机状态监视模块设置在虚拟机监控器内部，虚拟机状态监视模块使用访问控制初始化模块设置的安全钩子函数监测虚拟机启动事件和关闭事件，当发生一个虚拟机启动事件时，虚拟机状态监视模块获得该虚拟机的 ID 号和敏感标签，保存在虚拟机监控器内部，为该虚拟机创建一个空的当前访问集合 b，当发生一个虚拟机关闭事件时，虚拟机状态监视模块清除该虚拟机在虚拟机监控器内部的 ID 号、敏感标签和当前访问集合 b；

访问判定模块设置在虚拟机监控器内部，访问判定模块使用访问控制初始化模块设置的安全钩子函数监测虚拟机之间通信和资源共享的事件，判断作为主体的虚拟机和作为客体的虚拟机的敏感标签和访问矩阵是否满足敏感标签安全特性和访问矩阵安全特性，如果满足则允许作为主体的虚拟机访问作为客体的虚拟机，当发生作为主体的虚拟机结束一次对作为客体的虚拟机的访问时，访问判定模块从作为主体的虚拟机的当前访问集合 b 中删除这次访问的记录；

安全管理协助模块设置在虚拟机监控器内部，安全管理协助模块在虚拟机安全信息管理模块使用敏感标签标识正在运行的虚拟机安全级别时，检查所有正在运行虚拟机的当前

访问集合 b 是否满足上述 6 个当前访问集合 b 的安全特性来判定虚拟机安全信息管理模块的操作能否成功；当虚拟机安全信息管理模块在某个作为主体的虚拟机对作为客体的虚拟机的访问类型集合中删除访问类型时，如果作为主体的虚拟机正在运行，安全管理协助模块从作为主体的虚拟机的当前访问集合 b 中删除作为主体的虚拟机对作为客体的虚拟机的访问类型；安全管理协助模块还为虚拟机安全信息管理模块提供接口，虚拟机安全信息管理模块使用这些接口把使用敏感标签标识虚拟机安全级别和设置访问矩阵的操作结果输出到虚拟机监控器内部。

3. 根据权利要求 2 所述的虚拟化环境中的强制访问控制装置，其特征是，所述虚拟机安全信息管理模块，其将建立的虚拟机的层次关系保存到可信虚拟机磁盘上的层次关系文件中，文件中的内容是使用树形数据结构描述层次关系的结果；将生成的敏感标签信息和访问矩阵的数据分开存储在可信虚拟机的磁盘文件中，其中，将敏感标签信息保存在虚拟机的敏感标签文件中，每个虚拟机都有自己的敏感标签文件，敏感标签文件除了包含该虚拟机的安全密级、安全范畴还有该虚拟机的 ID 号，ID 号是该虚拟机在访问矩阵中的索引，在该虚拟机被从系统中删除之前保持不变；虚拟机安全信息管理模块将访问矩阵的数据保存在访问矩阵文件中，整个系统只有一个访问矩阵文件，它是一个二进制文件，保存代表访问矩阵的一维有序数组的二进制形式；

虚拟机安全信息管理模块通过安全管理协助模块提供的接口将操作结果传输到虚拟机监控器内部，对于正在运行的虚拟机，虚拟机安全信息管理模块把使用敏感标签标识虚拟机的安全级别和设置访问矩阵的操作结果均输出到虚拟机监控器内部；对于不在运行状态的虚拟机，虚拟机安全信息管理模块把设置访问矩阵的操作结果输出到虚拟机监控器内部，使用敏感标签标识虚拟机安全级别的操作结果不输出到虚拟机监控器内部，在虚拟机安全信息管理模块把操作结果输出到虚拟监控器之后，虚拟机与其他虚拟机通信时访问判定模块使用虚拟机安全信息管理模块更新过的敏感标签和访问矩阵做判定。

4. 根据权利要求 2 所述的虚拟化环境中的强制访问控制装置，其特征是，所述访问控制初始化模块，在虚拟机监控器启动时把访问矩阵文件中的数据从可信虚拟机的磁盘文件中加载到虚拟机监控器内部，然后遍历访问矩阵的一维数组，为数组中的每个元素创建一个链表节点，在链表节点中保存数组元素的内容，最后把所有链表节点连接成有序双向链表，以便于安全管理协助模块通过其为虚拟机安全信息管理模块提供的接口往矩阵中增加、删除元素；

访问控制初始化模块在虚拟机启动与关闭、虚拟机之间通信和资源共享的关键路径上设置安全钩子函数，当虚拟机启动、关闭和虚拟机之间通信和资源共享这些事件发生时安全钩子函数被执行，安全钩子函数的具体操作分别由虚拟机状态监视模块和访问判定模块实现，安全钩子函数的返回结果也分别由虚拟机状态监视模块和访问判定模块决定。

5. 根据权利要求 2 所述的虚拟化环境中的强制访问控制装置，其特征是，所述访问判定模块，当其使用访问控制初始化模块设置的安全钩子函数监测虚拟机之间通信和资源共享行为，当虚拟机之间通信和资源共享行为发生时，安全钩子函数首先获取本次行为的访问类型、作为主体的虚拟机 S 和作为客体的虚拟机 O 的敏感标签；其次查询访问矩阵中作为主体的虚拟机 S 对作为客体的虚拟机 O 的访问类型集合；再次使用安全钩子函数获取的信息判断作为主体的虚拟机和作为客体的虚拟机的敏感标签和访问矩阵是否满足敏感标

签安全特性和访问矩阵安全特性；最后如果判定结果为允许，则在作为主体的虚拟机当前访问集合 b 中添加一条访问记录，作为主体的虚拟机访问作为客体的虚拟机的过程继续进行，如果判定结果为不允许，则截断作为主体的虚拟机对作为客体的虚拟机的访问过程，并返回出错消息；

访问判定模块使用访问控制初始化模块设置的安全钩子函数监测虚拟机之间通信和资源共享行为结束，当此类事件发生时，安全钩子函数首先获取作为主体的虚拟机和作为客体的虚拟机的 ID 号，以及本次访问的类型信息，然后在作为主体的虚拟机当前访问集合 b 中删除本次访问的记录。

6. 根据权利要求 2 所述的虚拟化环境中的强制访问控制装置，其特征是，所述安全管理协助模块，其在虚拟机安全信息管理模块使用敏感标签标识正在运行的虚拟机安全级别时，遍历所有正在运行的虚拟机的当前访问集合 b，检查是否满足上述 6 个当前访问集合 b 的安全特性，如果有任一安全特性不满足，则返回失败消息，虚拟机安全信息管理模块操作失败；如果 6 个安全特性都满足，则返回成功消息，虚拟机安全信息管理模块操作成功，虚拟机安全信息管理模块操作成功之后立即通过安全管理协助模块提供的接口把被标识虚拟机的敏感标签输出到虚拟机监控器内部，更新虚拟机监控器内部被虚拟机安全信息管理模块操作成功的虚拟机的敏感标签，如果被虚拟机安全信息管理模块标识的虚拟机没有处于运行状态，则在标识的过程中不需要与安全管理协助模块交互，标识后该虚拟机的敏感标签不需要立即输出到虚拟机监控器内部；

安全管理协助模块在虚拟机安全信息管理模块设置访问矩阵时，如果虚拟机安全信息管理模块的操作是在作为主体的虚拟机 S 访问作为客体的虚拟机 O 的访问类型集合中删除访问类型 x 并且作为主体的虚拟机 S 所代表的另一虚拟机正在运行，则需要从作为主体的虚拟机 S 所代表虚拟机的当前访问集合 b 中删除关于 S 以类型 x 访问作为客体的虚拟机 O 的记录，如果虚拟机安全信息管理模块的操作是在作为主体的虚拟机 S 访问作为客体的虚拟机 O 的访问类型集合中添加访问类型 x，则安全管理协助模块不需要做附加操作。

虚拟化环境中的强制访问控制方法及装置

技术领域

[0001] 本发明涉及的是一种计算机应用技术领域的方法及装置，具体是一种虚拟化环境中的强制访问控制方法及装置。

背景技术

[0002] 虚拟化技术是当前信息技术行业最为热门的技术，应用虚拟化技术可以在下述几个方面带来巨大好处：1、整合服务器，将计算机系统部署到虚拟机中可以提高硬件设备利用率，降低运营成本；2、利用资源虚拟化提升服务质量，减少系统下线时间；3、缩减 IT 基础设置的准备时间，提升 IT 投资的灵活性，促进按需配置；4、快速提供测试和开发环境，提高开发效率；5、将遗留的操作系统和应用程序迁移到虚拟机中，保护历史投资；6、利用服务器的虚拟化能力提供标准化的企业桌面环境，提高企业 IT 设备的利用率和可管理性。

[0003] 虚拟机监控器是虚拟化技术的核心，虚拟机运行在虚拟机监控器之上。虚拟机监控器主要功能包括：1、管理物理硬件资源；2、为运行在它上面的虚拟机提供虚拟的硬件资源；3、为在它上面运行的多个虚拟机提供互相隔离的运行环境，使得多个虚拟机不能互相干扰对方运行；4、为运行在它上面的虚拟机提供虚拟机之间通信和资源共享支持。

[0004] 目前信息技术行业的各大公司不断加大投入推动虚拟化技术发展，携手制定虚拟化技术应用的标准，不同虚拟机之间的通信和共享资源越来越受到重视。为了建立一个安全可信的虚拟化应用环境，必须对虚拟机之间通信和资源共享实施访问控制。

[0005] 在一次通信和资源共享的操作过程中处于施动者地位的对象称为主体，处于受动者地位的对象称为客体。在虚拟化场景中每个虚拟机在通信过程中既可能是主体也可能是客体，根据通信过程中数据的流向判断虚拟机是主体还是客体。在计算机系统上执行访问控制的基本思想是在主体访问客体关键路径中插入用于安全目的的函数，这样的函数通常称为安全钩子函数 (security hooks)。当主体访问客体时安全钩子函数被执行，它检查主体和客体的安全信息依据特定的安全策略判定主体是否可以访问客体，如果可以访问则它记录相关信息后主体访问客体的过程继续进行，如果不可以访问则它截断主体访问客体的过程，并返回出错消息。安全钩子函数做判定时所采用的安全策略是访问控制的核心内容。

[0006] 经对现有技术文献的检索发现，以 Reiner Sailer 为主提出控制虚拟机之间通信和资源共享的方法 (Reiner Sailer, Trent Jaeger, Enriquillo Valdez.Building a MAC-based Security Architecture for the Xen Opensource Hypervisor,(在Xen开源虚拟机监控器上建立一种基于强制访问控制的安全架构)RC23629(W0506-051)June 8,2005. IBM Research Report.)。该方法是基于中国墙 (Chinese wall) 和简单类型加强 (Simple Type Enforcement) 策略，该方法为虚拟化环境中的虚拟机和资源设置不同的标签，标签可以代表不同的组织或部门，同时设置冲突的标签集合。当两个虚拟机上的标签处于冲突集合中时，它们不能同时运行，当两个虚拟机具有相同的标签时，双方可以通信和共享资源。该方法存在如下问题：1) 该方法对通信和资源共享的控制力度较大，不控制具体的通信和资源共享类型；2) 假设使用不同的标签代表不同的安全级别，不同安全级别的虚拟机之间

无法通信和共享资源。因此该方法不适用于多级安全环境。

发明内容

[0007] 本发明的目的是为了克服上述现有技术的不足，提供一种虚拟化环境中的强制访问控制方法及装置，以敏感标签和访问矩阵为核心，包括在虚拟机监控器内的实施强制访问控制，可以满足多级安全环境的要求，包括：用敏感标签标识单个虚拟机安全级别、在访问矩阵中表达作为主体的虚拟机对作为客体的虚拟机的访问类型、在虚拟机监控器内根据敏感标签和访问矩阵中的信息控制虚拟机之间通信和资源共享。

[0008] 本发明是通过如下技术方案实现的。

[0009] 本发明涉及一种虚拟化环境中的强制访问控制方法，包括如下步骤：

[0010] 步骤一，在虚拟化场景中指定一个虚拟机作为具有安全管理权限的可信虚拟机，并以这个可信虚拟机为根，其他虚拟机为可信虚拟机的子节点建立层次关系，除可信虚拟机之外的其他所有虚拟机处于同等的地位；

[0011] 步骤二，可信虚拟机使用敏感标签对其他单个虚拟机安全级别进行标识，所述敏感标签包括安全密级和安全范畴；

[0012] 步骤三，建立可信虚拟机的访问矩阵，访问矩阵中记录每个虚拟机对其他虚拟机的访问类型集合，访问类型包括：只读、只写和读写三种，访问矩阵中的数据在虚拟机监控器启动时被加载到虚拟机监控器内部；

[0013] 步骤四，当一个虚拟机启动时，把它的 ID 号、敏感标签作为参数传入虚拟机监控器内部，在虚拟机监控器内部记录这些信息，并为该虚拟机建立一个当前访问集合 b，对所有其他虚拟机的访问类型；；

[0014] 步骤五，当通信或资源共享行为发生时，检查作为主体的虚拟机和作为客体的虚拟机的敏感标签和访问矩阵是否满足敏感标签安全特性和访问矩阵安全特性，如果满足则允许作为主体的虚拟机访问作为客体的虚拟机，否则不允许作为主体的虚拟机访问作为客体的虚拟机并返回出错消息；

[0015] 所述敏感标签安全特性，是指：当作为主体的虚拟机对作为客体的虚拟机进行只读访问时，作为主体的虚拟机的敏感标签必须支配作为客体的虚拟机的敏感标签；当作为主体的虚拟机对作为客体的虚拟机进行只写访问时，作为主体的虚拟机的敏感标签必须被作为客体的虚拟机的敏感标签支配；当作为主体的虚拟机对作为客体的虚拟机进行读写访问时，作为主体的虚拟机的敏感标签必须等于作为客体的虚拟机的敏感标签；

[0016] 所述访问矩阵安全特性，是指当作为主体的虚拟机对作为客体的虚拟机进行只读、只写或者读写类型的访问时，其访问类型存在于访问矩阵中代表作为主体的虚拟机对作为客体的虚拟机的访问类型集合中。

[0017] 步骤六，当步骤五返回的结果是允许访问时，在作为主体的虚拟机的当前访问集合 b 中加入一条这次访问的记录；

[0018] 步骤七，当作为主体的虚拟机结束对作为客体的虚拟机的一次访问时，从当前访问集合 b 中删除关于这次访问的记录。

[0019] 步骤二中，所述虚拟机的敏感标签，其中的安全密级采用数值形式，数值越大密级越高，安全范畴为特定访问权限的集合，集合中的每个元素代表一项特定的访问权限，两个

敏感标签之间的关系是支配与被支配、等于或者不可比较的关系。当敏感标签 f_1 和 f_2 做比较时，如果 f_1 的安全密级高于 f_2 的安全密级同时 f_1 的安全范畴包含 f_2 的安全范畴，则 f_1 支配 f_2，或者说 f_2 被 f_1 支配，如果 f_1 的安全密级与 f_2 的安全密级相等并且 f_1 的安全范畴与 f_2 的安全范畴相等则 f_1 等于 f_2，否则 f_1 和 f_2 是不可比较的。

[0020] 步骤二中，所述对其他单个虚拟机的安全级别进行标识，具体如下：如果被标识的虚拟机没有敏感标签，则直接使用敏感标签标识该虚拟机的安全级别；如果被标识的虚拟机已经具有敏感标签，则使用新敏感标签重新标识该虚拟机的安全级别，即调整该虚拟机的安全级别，如果标识安全级别时，被标识的虚拟机正在运行则需要所有正在运行虚拟机的当前访问集合 b 同时满足下述 6 个当前访问集合 b 安全特性，标识操作才能成功：

[0021] ①被标识的虚拟机的新敏感标签能够支配所有其他虚拟机的当前访问集合 b 中对该虚拟机进行只写访问虚拟机的敏感标签；

[0022] ②当前访问集合 b 中对被标识的虚拟机进行只读访问的所有其他虚拟机的敏感标签能够支配该虚拟机的新敏感标签；

[0023] ③当前访问集合 b 中对被标识的虚拟机进行读写访问的所有其他虚拟机的敏感标签等于该虚拟机的新敏感标签；

[0024] ④被标识的虚拟机的新敏感标签必须支配它自己的当前访问集合 b 中所有被该虚拟机只读访问的其他虚拟机的敏感标签；

[0025] ⑤在被标识的虚拟机自己的当前访问集合 b 中所有被它只写访问的其他虚拟机敏感标签能够支配该虚拟机的新敏感标签；

[0026] ⑥被标识的虚拟机的新敏感标签等于它自己的当前访问集合 b 中所有被该虚拟机读写访问的其他虚拟机敏感标签。

[0027] 步骤三中，所述每个虚拟机对其他虚拟机的访问类型集合，其中不能设置其他虚拟机对可信虚拟机的访问类型集合，即所有其他虚拟机不能作为主体与可信虚拟机通信，可信虚拟机不能作为客体出现在通信过程中。

[0028] 步骤三中，所述每个虚拟机对其他虚拟机的访问类型集合，是指向访问类型集合中增加访问类型，或者是从访问类型集合中删除访问类型，前者是授予作为主体的虚拟机对作为客体的虚拟机的某种访问类型，后者是撤销作为主体的虚拟机对作为客体的虚拟机的某种访问类型。

[0029] 步骤五中，所述访问控制过程，包括如下三种情况：

[0030] ①当作为主体的虚拟机对作为客体的虚拟机做只读访问时，需要同时满足两个安全特性允许作为主体的虚拟机只读访问作为客体的虚拟机：敏感标签安全特性：作为主体的虚拟机是可信虚拟机或者作为主体的虚拟机的敏感标签支配作为客体的虚拟机的敏感标签；访问矩阵安全特性：作为主体的虚拟机在访问矩阵中具有对作为客体的虚拟机的只读访问类型；

[0031] ②当作为主体的虚拟机对作为客体的虚拟机做只写访问时，需要同时满足两个安全特性允许作为主体的虚拟机只写访问作为客体的虚拟机：敏感标签安全特性：作为主体的虚拟机是可信虚拟机或者作为客体的虚拟机的敏感标签支配作为主体的虚拟机的敏感标签；访问矩阵安全特性：作为主体的虚拟机在访问矩阵中具有对作为客体的虚拟机的只写访问类型；

[0032] ③当作为主体的虚拟机对作为客体的虚拟机做读写访问时，需要同时满足两个安全特性允许作为主体的虚拟机读写访问作为客体的虚拟机：敏感标签安全特性：作为主体的虚拟机是可信虚拟机或者作为主体的虚拟机的敏感标签等于作为客体的虚拟机的敏感标签；访问矩阵安全特性：作为主体的虚拟机在访问矩阵中具有对作为客体的虚拟机的读写访问类型。

[0033] 步骤五中，所述访问控制过程，如果在通信过程中可信虚拟机是作为主体的虚拟机，则不受两个条件的约束，即可信虚拟机可以以任意类型访问其他作为客体的虚拟机。

[0034] 步骤六中，所述作为主体的虚拟机的当前访问集合 b，负责记录每次访问的信息，记录的信息包括在这次访问被作为主体的虚拟机访问的作为客体的虚拟机的 ID 号和访问类型。

[0035] 本发明还涉及一种虚拟化环境中的强制访问控制装置，包括：虚拟机安全信息管理模块 (Virtual Machine Security Information Manager，简称 VMSIM 模块)、访问控制初始化模块 (Access Control Initialization，简称 ACI 模块)、虚拟机状态监视模块 (Virtual Machine State Watcher，简称 VMSW 模块)、访问判定模块 (Access Decision-maker，简称 AD 模块)、安全管理协助模块 (Security Managing Assistant，简称 SMA 模块)，其中，

[0036] 虚拟机安全信息管理模块设置在可信虚拟机中，将其他虚拟机作为可信虚拟机的子节点，从而建立起虚拟机的层次关系，同时，使用敏感标签标识其他虚拟机的安全级别，在访问矩阵中设置每个虚拟机对其他虚拟机的访问类型集合，并将上述操作结果一方面保存到可信虚拟机的磁盘文件中，另一方面输出到虚拟机监控器内部；

[0037] 访问控制初始化模块设置在虚拟机监控器内部，访问控制初始化模块在虚拟机监控器启动的过程中，从可信虚拟机的磁盘中把访问矩阵加载到虚拟机监控器的内部，在虚拟机启动与关闭、虚拟机之间通信和资源共享的关键路径上设置安全钩子函数，供虚拟机状态监视模块和访问判定模块使用；

[0038] 虚拟机状态监视模块设置在虚拟机监控器内部，虚拟机状态监视模块使用访问控制初始化模块设置的安全钩子函数监测虚拟机启动事件和关闭事件，当发生一个虚拟机启动事件时，虚拟机状态监视模块获得该虚拟机的 ID 号和敏感标签，保存在虚拟机监控器内部，为该虚拟机创建一个空的当前访问集合 b，当发生一个虚拟机关闭事件时，虚拟机状态监视模块清除该虚拟机在虚拟机监控器内部的 ID 号、敏感标签和当前访问集合 b；

[0039] 访问判定模块设置在虚拟机监控器内部，访问判定模块使用访问控制初始化模块设置的安全钩子函数监测虚拟机之间通信和资源共享的事件，判断作为主体的虚拟机和作为客体的虚拟机的敏感标签和访问矩阵是否满足敏感标签安全特性和访问矩阵安全特性，如果满足则允许作为主体的虚拟机访问作为客体的虚拟机，当发生作为主体的虚拟机结束一次对作为客体的虚拟机的访问时，访问判定模块从作为主体的虚拟机的当前访问集合 b 中删除这次访问的记录；

[0040] 安全管理协助模块设置在虚拟机监控器内部，安全管理协助模块在虚拟机安全信息管理模块使用敏感标签标识正在运行的虚拟机安全级别时，检查所有正在运行虚拟机的当前访问集合 b 是否满足 6 个当前访问集合 b 安全特性来判定虚拟机安全信息管理模块的操作能否成功；当虚拟机安全信息管理模块在某个作为主体的虚拟机对作为客体的虚拟机

的访问类型集合中删除访问类型时，如果作为主体的虚拟机正在运行，安全管理协助模块从作为主体的虚拟机当前访问集合 b 中删除作为主体的虚拟机对作为客体的虚拟机的访问类型；安全管理协助模块还为虚拟机安全信息管理模块提供接口，虚拟机安全信息管理模块使用这些接口把使用敏感标签标识虚拟机安全级别和设置访问矩阵的操作结果输出到虚拟机监控器内部。

[0041] 所述虚拟机安全信息管理模块，其将建立的虚拟机的层次关系保存到可信虚拟机磁盘上的层次关系文件中，文件中的内容是使用树形数据结构描述层次关系的结果。

[0042] 所述虚拟机安全信息管理模块，其将生成的敏感标签信息和访问矩阵的数据分开存储在可信虚拟机的磁盘文件中，其中，将敏感标签信息保存在虚拟机的敏感标签文件中，每个虚拟机都有自己的敏感标签文件，敏感标签文件除了包含该虚拟机的安全密级、安全范畴还有该虚拟机的 ID 号，ID 号是该虚拟机在访问矩阵中的索引，在该虚拟机被从系统中删除之前保持不变；虚拟机安全信息管理模块将访问矩阵的数据保存在访问矩阵文件中，整个系统只有一个访问矩阵文件，它是一个二进制文件，保存代表访问矩阵的一维有序数组的二进制形式。

[0043] 所述虚拟机安全信息管理模块，其通过安全管理协助模块提供的接口将操作结果传输到虚拟机监控器内部。对于正在运行的虚拟机，虚拟机安全信息管理模块把使用敏感标签标识虚拟机的安全级别和设置访问矩阵的操作结果均输出到虚拟机监控器内部；对于不在运行状态的虚拟机，虚拟机安全信息管理模块把设置访问矩阵的操作结果输出到虚拟机监控器内部，使用敏感标签标识虚拟机安全级别的操作结果不输出到虚拟机监控器内部。在虚拟机安全信息管理模块把操作结果输出到虚拟监控器之后，虚拟机与其他虚拟机通信时访问判定模块使用虚拟机安全信息管理模块更新过的敏感标签和访问矩阵做判定；

[0044] 所述访问控制初始化模块，在虚拟机监控器启动时把访问矩阵文件中的数据从可信虚拟机的磁盘文件中加载到虚拟机监控器内部，然后遍历访问矩阵的一维数组，为数组中的每个元素创建一个链表节点，在链表节点中保存数组元素的内容，最后把所有链表节点连接成有序双向链表，以便于安全管理协助模块通过为虚拟机安全信息管理模块提供的接口往矩阵中增加、删除元素。

[0045] 所述访问控制初始化模块，其在虚拟机监控内部虚拟机启动、关闭和虚拟机之间通信和资源共享的关键路径上设置安全钩子函数，当虚拟机启动、关闭和虚拟机之间通信和资源共享这些事件发生时安全钩子函数被执行。安全钩子函数的具体操作分别由虚拟机状态监视模块和访问判定模块实现，安全钩子函数的返回结果也分别由虚拟机状态监视模块和访问判定模块决定。

[0046] 所述访问判定模块，其使用访问控制初始化模块设置的安全钩子函数监测虚拟机之间通信和资源共享行为。当发生虚拟机之间通信和资源共享行为时，安全钩子函数首先获取本次行为的访问类型、作为主体的虚拟机 S 和作为客体的虚拟机 O 的敏感标签；其次查询访问矩阵中作为主体的虚拟机 S 对作为客体的虚拟机 O 的访问类型集合；再次使用安全钩子函数获取的信息判断作为主体的虚拟机和作为客体的虚拟机的敏感标签和访问矩阵是否满足敏感标签安全特性和访问矩阵安全特性；最后如果判定结果为允许，则在作为主体的虚拟机当前访问集合 b 中添加一条访问记录，作为主体的虚拟机访问作为客体的虚拟

机的过程继续进行，如果判定结果为不允许，则截断作为主体的虚拟机对作为客体的虚拟机的访问过程，并返回出错消息。当虚拟机之间通信和资源共享行为结束时，安全钩子函数首先获取作为主体的虚拟机和作为客体的虚拟机的 ID 号，以及本次行为的访问类型信息，然后在作为主体的虚拟机的当前访问集合 b 中删除本次访问的记录。

[0047] 所述安全管理协助模块，其在虚拟机安全信息管理模块使用敏感标签标识正在运行的虚拟机安全级别时，遍历所有正在运行的虚拟机的当前访问集合 b，检查是否满足上述 6 个当前访问集合 b 安全特性，如果有任一安全特性不满足，则返回失败消息，虚拟机安全信息管理模块操作失败；如果 6 个安全特性都满足，则返回成功消息，虚拟机安全信息管理模块操作成功，虚拟机安全信息管理模块操作成功之后立即通过安全管理协助模块提供的接口把被标识虚拟机的敏感标签输出到虚拟机监控器内部，更新虚拟机监控器内部被虚拟机安全信息管理模块操作成功的虚拟机的敏感标签。如果被虚拟机安全信息管理模块标识的虚拟机没有处于运行状态，则在标识的过程中不需要与安全管理协助模块交互，标识后该虚拟机的敏感标签不需要立即输出到虚拟机监控器内部。

[0048] 所述安全管理协助模块，在虚拟机安全信息管理模块设置访问矩阵时，如果虚拟机安全信息管理模块的操作是在作为主体的虚拟机 S 访问作为客体的虚拟机 O 的访问类型集合中删除访问类型 x 并且作为主体的虚拟机 S 所代表的虚拟机正在运行，则需要从作为主体的虚拟机 S 所代表虚拟机的当前访问集合 b 中删除关于 S 以类型 x 访问作为客体的虚拟机 O 的记录，如果虚拟机安全信息管理模块的操作是在作为主体的虚拟机 S 访问作为客体的虚拟机 O 的访问类型集合中添加访问类型 x，则安全管理协助模块不需要做附加操作。

[0049] 与现有技术相比，本发明具有如下有益效果：

[0050] 1、本发明区分虚拟机之间通信和资源共享的访问类型，访问判定模块做访问判定时需要考虑具体的访问类型。一个作为主体的虚拟机可能有对一个作为客体的虚拟机的某种访问类型，但是没有全部访问类型；反之一个作为主体的虚拟机可能没有对一个作为客体的虚拟机特定的某种访问类型，但是有其他的访问类型。而现有技术不区分访问类型，访问控制只考虑两种情况：①允许虚拟机之间任意类型的通信和资源共享；②不允许虚拟机之间任意类型的通信和资源共享。针对具体的访问类型做访问控制的特点使得本发明比现有技术更灵活，可以更好的满足虚拟机技术应用的安全需求。

[0051] 2、本发明在保证不破坏信息机密性的前提下使得不同安全级别的虚拟机之间可以通信和资源共享，可以促进多级安全环境下虚拟机技术的应用。而现有技术可以采用标签来标识虚拟机不同的安全级别，没有相同标签的虚拟机之间不能通信和资源共享。在多级安全的虚拟化环境中现有技术只能阻止不同安全级别的虚拟机之间通信和资源共享。

附图说明

[0052] 图 1 是本发明实施例中虚拟机之间的层次关系示意图；

[0053] 图 2 是发明实施例中 Xen 虚拟机监控器与物理硬件、虚拟机操作系统的关系；

[0054] 图 3 是本发明装置的系统结构框图；

[0055] 图 4 是本发明的实施例中虚拟机监控器 Xen 的两个 domain 在通信过程中使用共享内存交换数据示意图；

[0056] 图 5 本发明实施例中虚拟机安全信息管理模块与安全管理协助模块之间通信机

制示意图；

[0057] 图 6 本实施例中访问判定模块做访问控制的流程图。

具体实施方式

[0058] 下面结合附图对本发明的实施例作详细说明：本实施例在以本发明技术方案为前提下进行实施，给出了详细的实施方式和具体的操作过程，但本发明的保护范围不限于下述的实施例。

[0059] 如图 1 所示，是本实施例的虚拟机层次关系，可信虚拟机处于层次关系的根节点上，其他虚拟机都是根节点的儿子节点。

[0060] 本实施例是在虚拟机监控器 Xen 上进行实施的。如图 2 所示，Xen 虚拟机监控器是剑桥大学计算机实验室开发的一个开源虚拟机监控器项目，Xen 虚拟机监控器与物理硬件、虚拟机 domain 操作系统、应用程序的关系，Xen 虚拟机监控器直接控制硬件资源，为在它之上的 domain 提供虚拟资源，隔离各个 domain 操作系统的执行环境，为 domain 之间提供通信和资源共享机制的支持。Xen 虚拟机监控器除了提供上述功能之外，还为 domain 操作系统提供超级调用 (Hypercall) 调用，domain 操作系统通过这类调用可以要求 Xen 虚拟机监控器完成某些不能由操作系统自身执行的操作，例如修改内存页表，修改虚拟机监控器内部的数据。

[0061] Xen 虚拟机监控器提供的虚拟机 domain 之间通信机制有事件通道 (event channel) 和共享内存 (grant table) 两种，具体如下：

[0062] 事件通道是两个 domain 之间同步的方法，一个事件通道由两个二进制位 (bit) 表示，其中一位表示事件提交 (pending) 状态，当该位被置为 1 时将调用 domain 事先注册的事件处理函数来处理该事件。另一位表示通道掩码 (mask)，当该位被置为 1 时，domain 暂时屏蔽该事件通道的事件处理。在半虚拟化的 domain 里面事件通道类似于软中断机制；

[0063] 共享内存是 domain 之间传送数据的方法，domain 可以在 Xen 虚拟机监控器的帮助下将属于自己的内存块授权 (grant) 另外一个 domain 访问或者将属于自己的内存块所有权传送 (transfer) 给另外一个 domain，当一个 domain 将属于自己的内存块授权给另一个 domain 时，两个 domain 都可以访问到该块内存，在操作完成后可以撤销授权；当一个 domain 将内存块传送所有权给另一个 domain 之后，它自身不能再访问该内存，同时失去对该内存的控制。

[0064] 在本实施例中建立事件通道和发送事件通知访问判定模块不检查具体的访问类型，只要 domain 之间在访问矩阵中是可以通信的则双方可以建立事件通道并互相发送事件通知，domain 之间的共享内存块做访问类型的解释，如图 4 所示，domain-1 共享一个属于自己的内存块给 domain-2，domain-2 把这块内存映射到自己的内存地址空间，然后对这块内存进行某种类型的操作，称这块内存为共享内存。在这次通信过程中 domain-2 被认为是主体，domain-1 被认为是客体，domain-2 对共享内存的操作等同于对 domain-1 的操作，访问类型由 domain-2 对共享内存的操作决定：

[0065] 例如 domain-2 对共享内存做只读操作 (read，在一次访问中只有读操作，没有写操作)，则访问类型是只读 (r)；

[0066] domain-2 对共享内存做读写操作 (write，在一次访问中既有读操作又有写操

作），则访问类型是读写（w）；

[0067] domain-2 对共享内存做只写操作（append，在一次访问中只有写操作，没有读操作），则访问类型是只写（a），此处的只写操作指的是只往共享内存中写，不读取共享内存的内容，至于写在什么位置不做要求，更不要求按顺序写在共享内存的末尾。

[0068] 本实施例涉及一种虚拟化环境中的强制访问控制方法，包括如下步骤：

[0069] 步骤一，在虚拟化场景中指定一个虚拟机作为具有安全管理权限的可信虚拟机，并以这个可信虚拟机为根，其他虚拟机为可信虚拟机的子节点建立层次关系，除可信虚拟机之外的其他所有虚拟机处于同等的地位；

[0070] 本实施例中，在 Xen 虚拟化环境中虚拟机被称为 domain，其中具有管理其他 domain 的权限，称之为虚拟机 domain-0，指定 domain-0 作为可信虚拟机和虚拟机层次关系的根，其他 domain 都是 domain-0 的儿子节点。

[0071] 步骤二，可信虚拟机使用敏感标签对单个虚拟机安全级别进行标识，所述敏感标签包括安全密级和安全范畴；

[0072] 在本实施列中，安全密级集合为 $C = \{C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8\}$，$C_1 > C_2 > \cdots > C_8$，定义 $K = \{K_1, K_2, K_3, \cdots, K_{16}\}$ 的任一子集为一个安全范畴，安全密级用 3 位二进制位表示，安全范畴用 16 位二进制位表示。因为安全密级之间的大小关系可以直接用数值大小做比较，所以定义 C_1 的二进制表示为 111，C_2 的二进制表示为 110，…，C_8 的二进制表示为 000，表示安全范畴的 16 位二进制位分别表示是否具有特定访问权限 K_1，K_2，…，K_{16}，其中第 i 位（$1 \leqslant i \leqslant 16$）为 1 代表有特定访问权限 K_i，为 0 代表没有特定访问权限 K_i。

[0073] 步骤三，可信虚拟机建立访问矩阵文件，访问矩阵文件中记录每个虚拟机对其他虚拟机的访问类型集合，访问类型包括：只读、只写和读写三种，访问矩阵文件中的数据在虚拟机监控器启动时被加载到虚拟机监控器内部；

[0074] 本实施例中，访问矩阵文件保存在 domain-0 的磁盘中，访问矩阵文件是一个二进制文件，保存一个一维有序数组，定义单个数组元素为一个五元组（SID，OID，R，A，W），其中 SID 为作为主体的虚拟机的 ID 号（Identification），OID 为作为客体的虚拟机的 ID 号，R 的值为 1 表示有访问类型 r，为 0 表示没有访问类型 r；A 的值为 1 表示有访问类型 a，为 0 表示没有访问类型 a；W 的值为 1 表示有访问类型 w，为 0 表示没有访问类型 w；数组按照关键字（SID，OID）的值升序排序，作为主体的虚拟机的 ID 号和作为客体的虚拟机的 ID 号分别等于它们所代表的 domain ID 号，domain ID 号采用 13 位二进制位表示，R、A 和 W 分别采用 1 位二进制位表示，共计 29 位二进制位表达一个五元组。

[0075] 上述 domain ID 号采用 13 位二进制位表示，安全密级采用为 3 位二进制位表示，安全范畴采用 16 位二进制位表示是为了符合在 Xen 虚拟机监控器上每个 domain 启动时向虚拟机监控器传递一个 32 比特的整数参数的要求，在本实施例中这个 32 比特的整数参数表示 domain ID 号、安全密级和安全范畴。

[0076] 步骤四，当一个虚拟机启动时，把它的 ID 号、敏感标签作为参数传入虚拟机监控器内部，在虚拟机监控器内部记录这些信息，并为该虚拟机建立一个当前访问集合 b，记录该虚拟机作为主体的虚拟机时对所有其他虚拟机的访问类型；

[0077] 本实施例中，当前访问集合 b 中的元素为（OID，x）$x \in \{r, w, a\}$，OID 为作为客体的虚拟机的 ID 号，等于作为客体的 domain 的 ID 号。

[0078] 步骤五，当通信或资源共享行为发生时，检查作为主体的虚拟机和作为客体的虚拟机的敏感标签和访问矩阵是否满足敏感标签安全特性和访问矩阵安全特性，如果满足则允许作为主体的虚拟机访问作为客体的虚拟机，否则不允许作为主体的虚拟机访问作为客体的虚拟机并返回出错消息；

[0079] 所述敏感标签安全特性，是指：当作为主体的虚拟机对作为客体的虚拟机进行只读访问时，作为主体的虚拟机的敏感标签必须支配作为客体的虚拟机的敏感标签；当作为主体的虚拟机对作为客体的虚拟机进行只写访问时，作为主体的虚拟机的敏感标签必须被作为客体的虚拟机的敏感标签支配；当作为主体的虚拟机对作为客体的虚拟机进行读写访问时，作为主体的虚拟机的敏感标签必须等于作为客体的虚拟机的敏感标签；

[0080] 所述访问矩阵安全特性，是指当作为主体的虚拟机对作为客体的虚拟机进行只读、只写或者读写类型的访问时，其访问类型存在于访问矩阵中代表作为主体的虚拟机对作为客体的虚拟机的访问类型元素集合中。

[0081] 步骤六，当步骤五返回的结果是允许访问时，在作为主体的虚拟机的当前访问集合 b 中加入一条这次访问的记录；

[0082] 步骤七，当作为主体的虚拟机结束对作为客体的虚拟机的一次访问时，从当前访问集合 b 中删除关于这次访问的记录。

[0083] 如图 3 所示，本实施例涉及一种虚拟化环境中的强制访问控制装置，包括：虚拟机安全信息管理模块、访问控制初始化模块、虚拟机状态监视模块、访问判定模块、安全管理协助模块，访问控制初始化模块、虚拟机状态监视模块、访问判定模块和安全管理协助模块均设置在 Xen 虚拟机监控器的内部，其中：

[0084] 访问控制初始化模块在 Xen 启动过程中把访问矩阵从 domain-0 中加载到 Xen 中，在 domain 启动、关闭、domain 之间通信和资源共享的关键路径上添加安全钩子函数；

[0085] 访问判定模块控制 domain 间的通信和资源共享行为；

[0086] 安全管理协助模块协助虚拟机安全信息管理模块管理 domain 的安全信息；

[0087] 虚拟机安全信息管理模块设置在 domain-0 中，代表可信虚拟机管理管理 domain 的安全信息。

[0088] 所述访问控制初始化模块，其在 Xen 虚拟机监控器内部 domain 启动和关闭，事件通道与共享内存的建立、使用和关闭、资源共享等关键路径上设置安全钩子函数，监测 domain 启动或关闭，事件通道和共享内存的建立、使用与关闭，资源共享等事件的发生。

[0089] 所述访问控制初始化模块，其在 Xen 启动过程中把访问矩阵文件从 domain-0 中加载到 Xen 内部，然后遍历访问矩阵的一维数组，为数组中的每个元素创建一个链表节点，在链表节点中保存数组元素五元组 (SID，OID，R，A，W) 的各个分量值，最后把所有链表节点连接成有序双向链表，以便于安全管理协助模块通过为虚拟机安全信息管理模块提供的接口在矩阵中增加、删除元素。

[0090] 所述虚拟机状态监视模块，其在某个 domain 启动时，使用访问控制初始化模块设置的安全钩子函数读入上述 domain 启动时传入的 32 比特整数参数，在虚拟机状态监视模块内记录该 domain 的 ID 号和敏感标签，为该 domain 创建空的当前访问集合 b，查找该 domain 作为主体时对作为客体的 domain 的访问类型集合在访问矩阵中的起始位置，使用指针记录该位置以便于访问矩阵的查找。

[0091] 所述访问判定模块，当其使用访问控制初始化模块设置的安全钩子函数监测到作为主体的虚拟机 S 访问作为客体的虚拟机 O 的共享内存事件时，其做访问控制的流程如图 6 所示，访问判定模块首先检查访问类型，然后根据不同的类型做出判定。下面以访问类型为只读 (r) 为例说明具体的过程：

[0092] 1、访问判定模块找到访问矩阵，根据作为主体的虚拟机 ID 号和作为客体的虚拟机 ID 号在访问矩阵中查找访问类型 r，如果查找成功则继续后续步骤，否则拒绝作为主体的虚拟机 S 以类型 r 访问作为客体的虚拟机 O；

[0093] 2、访问判定模块比较作为主体的虚拟机 S 与作为客体的虚拟机 O 的安全密级，如果作为主体的虚拟机 S 的安全密级大于作为客体的虚拟机 O 的安全密级则继续后续步骤，否则拒绝作为主体的虚拟机 S 以类型 r 访问作为客体的虚拟机 O；

[0094] 3、访问判定模块比较作为主体的虚拟机 S 与作为客体的虚拟机 O 的安全范畴，如果作为主体的虚拟机 S 的安全范畴包含作为客体的虚拟机 O 的安全范畴则允许作为主体的虚拟机 S 以类型 r 访问作为客体的虚拟机 O，否则拒绝作为主体的虚拟机 S 以类型 r 访问作为客体的虚拟机 O。

[0095] 当访问判定模块允许作为主体的虚拟机 S 以类型 x 访问 O 之后，它在作为主体的虚拟机 S 代表的 domain 当前访问集合 b 中添加一条记录 (OID，x)。当访问控制初始化模块设置的安全钩子函数监测到作为主体的虚拟机 S 对作为客体的虚拟机 O 的这块共享内存操作结束、作为客体的虚拟机 O 撤销作为主体的虚拟机 S 对共享内存的访问授权时，访问判定模块将从作为主体的虚拟机 S 代表的 domain 的当前访问集合 b 中删除记录 (OID，x)。

[0096] 当访问控制初始化模块设置的安全钩子函数监测到 domain 关闭事件时，虚拟机状态监视模块将删除该 domain 的当前访问集合 b，清除虚拟监控器内部该 domain 的 ID 号和敏感标签信息。

[0097] 如图 5 所示，所述虚拟机安全信息管理模块，其设置在可信虚拟机 domain-0 内部，其具有调用 Xen 虚拟机监控器内部的安全管理协助模块的功能，一起完成 domain 的安全信息管理，虚拟机安全信息管理模块与安全管理协助模块之间的通信机制如下：domain-0 是一个 Linux 操作系统，虚拟机安全信息管理模块是一个运行在用户态的程序，当它调用安全管理协助模块的功能时，它首先使用用户态的 libxenctrl 程序库向运行在 domain-0 内核态的内核模块 privcmd 发送消息，privcmd 模块接收到来自它的消息后，通过超级调用 (Hypercall) 调用安全管理协助模块提供的接口函数管理 Xen 虚拟机监控器内部的 domain 敏感标签信息和访问矩阵。

[0098] 所述虚拟机安全信息管理模块，在 domain-0 中可以使用敏感标签标识其他 domain 的安全级别，在访问矩阵中授予或者撤销某个 domain 对其他 domain 的访问类型。虚拟机安全信息管理模块的操作结果除了保存在 domain-0 中的敏感标签文件和访问矩阵文件中外，还通过安全管理协助模块提供的接口传输到 Xen 虚拟机监控器内部。对于正在运行的 domain，虚拟机安全信息管理模块把使用敏感标签标识 domain 的安全级别和设置访问矩阵的操作结果均输出到 Xen 虚拟机监控器内部；对于不在运行状态的 domain，虚拟机安全信息管理模块把设置访问矩阵的操作结果输出到 Xen 虚拟机监控器内部，使用敏感标签标识 domain 安全级别的操作结果不输出到 Xen 虚拟机监控器内部。

[0099] 当虚拟机安全信息管理模块使用敏感标签标识正在运行 domain 的安全级别时，

安全管理协助模块需要遍历所有正在运行 domain 的当前访问集合 b，检查是否满足上述 6 个当前访问集合 b 安全特性，如果有任一安全特性不满足，则安全管理协助模块返回失败消息，虚拟机安全信息管理模块操作失败；如果 6 个安全特性都满足，则安全管理协助模块返回成功消息，虚拟机安全信息管理模块操作成功，并把被标识 domain 的敏感标签输出到虚拟监控器内部，立即更新 Xen 虚拟机监控器内部该 domain 的敏感标签。当虚拟机安全信息管理模块设置访问矩阵时，如果是在作为主体的虚拟机 S 访问作为客体的虚拟机 O 的访问类型集合中删除访问类型 x 并且作为主体的虚拟机 S 所代表的 domain 正在运行，则需要从作为主体的虚拟机 S 所代表 domain 的当前访问集合 b 中删除关于 S 以类型 x 访问作为客体的虚拟机 O 的记录；如果是在作为主体的虚拟机 S 访问作为客体的虚拟机 O 的访问类型集合中增加访问类型 x，则安全管理协助模块不需要修改作为主体的虚拟机 S 所代表 domain 的当前访问集合 b。当虚拟机安全信息管理设置作为主体的虚拟机 S 访问作为客体的虚拟机 O 的访问类型集合时，虚拟机安全信息管理模块除了把访问矩阵修改结果保存到访问矩阵文件中外，还需要同时把访问矩阵的修改结果输出到 Xen 虚拟机监控器内部。

[0100] 本实施例在多级安全虚拟化环境中可以更灵活的控制 domain 之间不同访问类型的通信和资源共享，不同安全级别的 domain 之间可以通信和资源共享。相比之下，现有技术（Reiner Sailer 等人提出的方法）不考虑虚拟机之间通信和资源共享具体的访问类型，无法让不同安全级别的虚拟机之间可以通信或资源共享。


可信虚拟机
虚拟机 1
虚拟机 2
.....
虚拟机 n-1
虚拟机 n

图 1

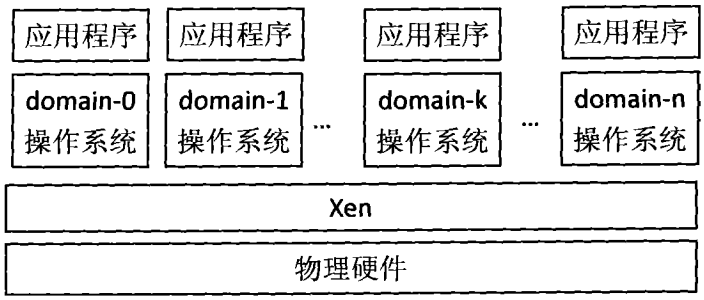

应用程序
应用程序
应用程序
应用程序
domain-0 操作系统
domain-1 操作系统
...
domain-k 操作系统
...
domain-n 操作系统
Xen
物理硬件

图 2

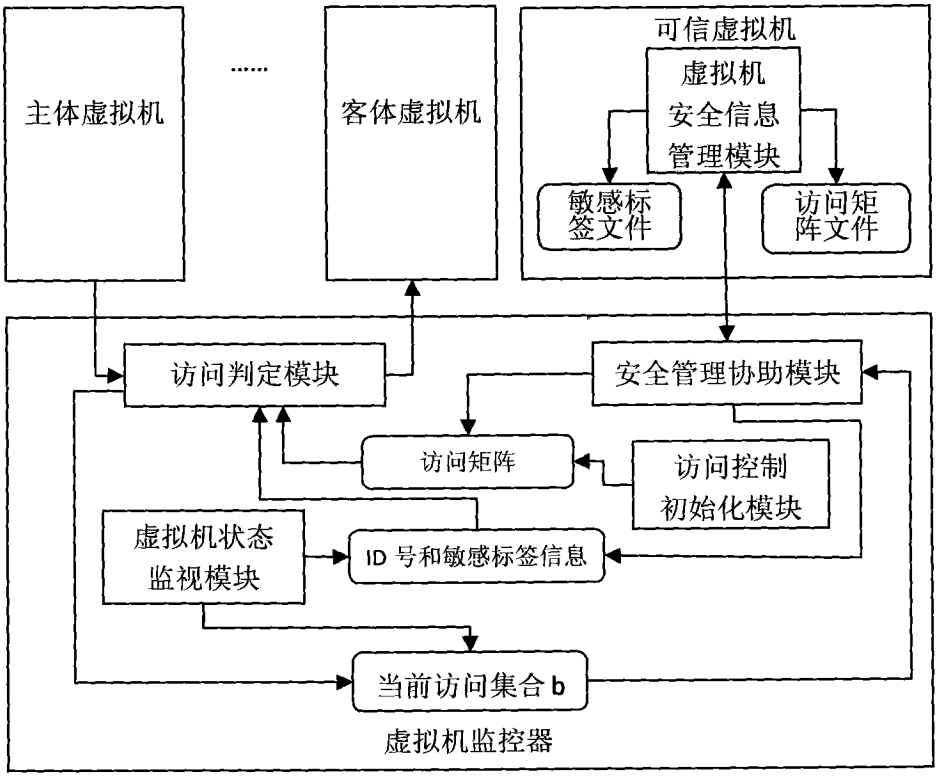

主体虚拟机
.....
客体虚拟机
可信虚拟机
虚拟机 安全信息 管理模块
敏感标签文件
访问矩阵文件
访问判定模块
安全管理协助模块
访问矩阵
访问控制 初始化模块
虚拟机状态 监视模块
ID 号和敏感标签信息
当前访问集合 b
虚拟机监控器

图 3

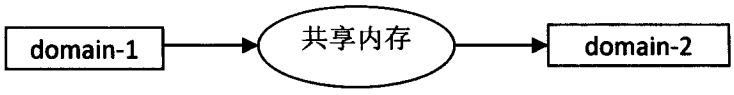

domain-1
共享内存
domain-2

图 4

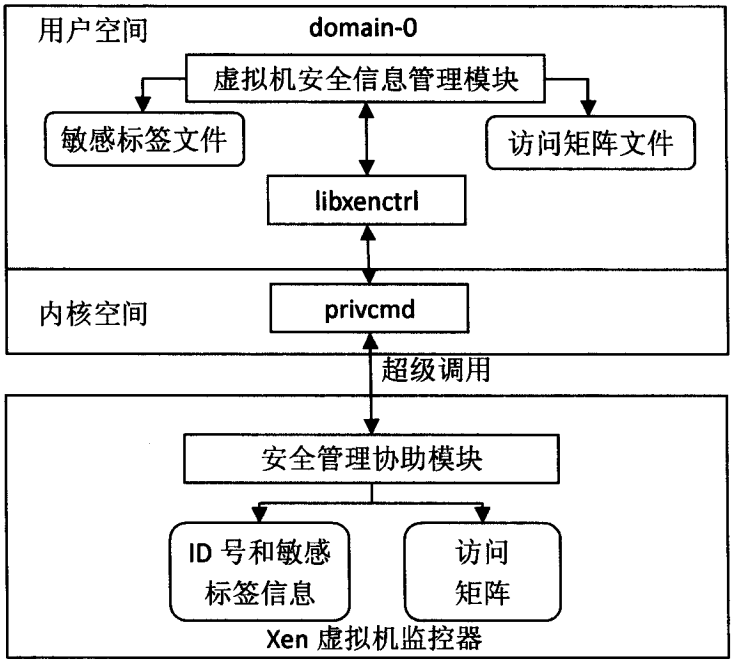

用户空间
domain-0
虚拟机安全信息管理模块
敏感标签文件
访问矩阵文件
libxenctrl
内核空间
privcmd
超级调用
安全管理协助模块
ID 号和敏感
标签信息
访问
矩阵
Xen 虚拟机监控器

图 5

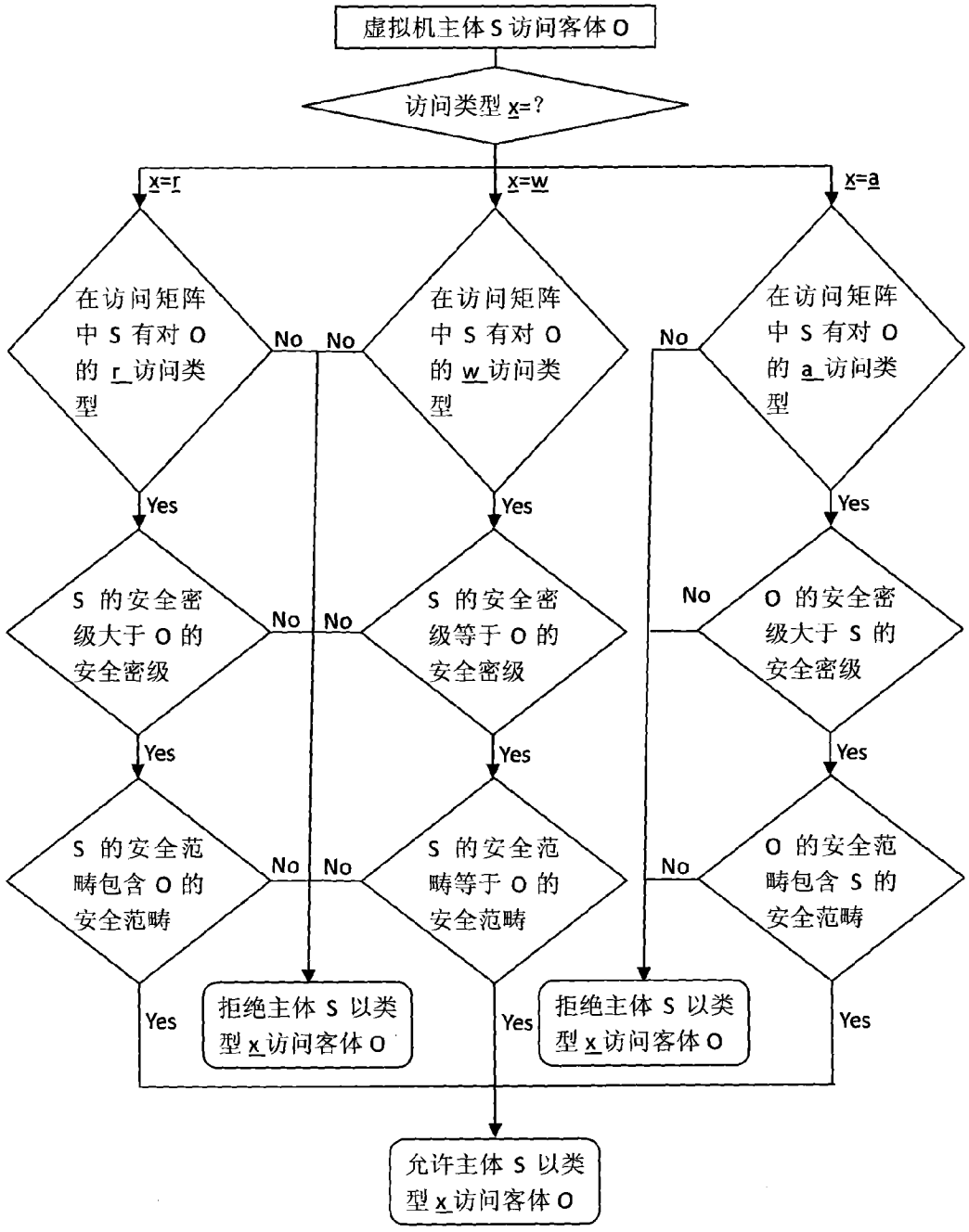

虚拟机主体 S 访问客体 O
访问类型 x=?
x=r
x=w
x=a
在访问矩阵中 S 有对 O 的 r 访问类型
在访问矩阵中 S 有对 O 的 w 访问类型
在访问矩阵中 S 有对 O 的 a 访问类型
No
Yes
S 的安全密级大于 O 的安全密级
S 的安全密级等于 O 的安全密级
O 的安全密级大于 S 的安全密级
S 的安全范畴包含 O 的安全范畴
S 的安全范畴等于 O 的安全范畴
O 的安全范畴包含 S 的安全范畴
拒绝主体 S 以类型 x 访问客体 O
允许主体 S 以类型 x 访问客体 O

图 6