(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 101310285 B
(45)授权公告日 2011.09.07

(21)申请号 200680043091.0
(22)申请日 2006.11.06
(30)优先权数据
05110841.3 2005.11.17 EP
(85)PCT申请进入国家阶段日
2008.05.19
(86)PCT申请的申请数据
PCT/IB2006/054115 2006.11.06
(87)PCT申请的公布数据
WO2007/057812 EN 2007.05.24
(73)专利权人 皇家飞利浦电子股份有限公司
地址 荷兰艾恩德霍芬
(72)发明人 W·F·J·方蒂恩
J·C·塔尔斯特拉 P·S·牛顿
K·J·G·霍尔特曼
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 李亚非 刘红
(51)Int.Cl.
G06F 21/00(2006.01)
G06F 21/24(2006.01)
(56)对比文件
JP 特开2005-235050 A,2005.09.02,全文.
US 2004/0148514 A1,2004.07.29,说明书第0010-0037段.
US 6092194 A,2000.07.18,说明书第2栏第66行至第7栏第45行.
CN 1366239 A,2002.08.28,全文.
审查员 丛珊

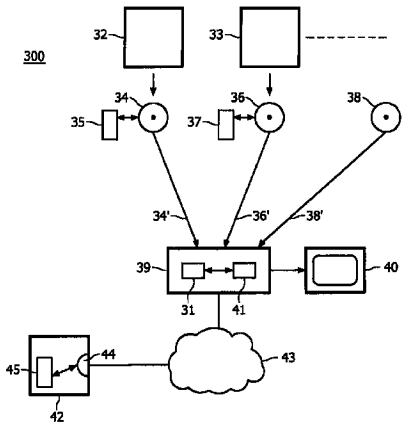
权利要求书 2 页 说明书 9 页 附图 3 页

(54)发明名称

用于管理访问控制的系统

(57)摘要

一种内容分发系统(300)具有根据预定义的数据访问格式的访问控制。该系统具有用于在记录载体(34)上提供内容数据和相关元数据的组织(32)、呈现设备(39)以及用于操纵所述内容数据和相关元数据的应用。根据所述预定义的数据访问格式设置对应于所述组织的访问策略,所述访问策略具有用于控制对所述呈现设备的资源以及对所述内容数据和相关元数据的访问的访问参数。执行符合所述组织的访问策略的组织应用(35)以便访问所述数据,同时根据所述组织的访问策略来访问所述呈现设备的资源。根据本发明,保持用户访问策略,其相对于所述组织的访问策略针对所述组织应用限制对所述呈现设备的资源的访问。基于附加的信任数据来调节所述用户访问策略,以便选择性地允许所述组织应用根据所述组织的访问策略来访问所述资源。因此,用户控制应用所具有的对所述呈现设备的资源的访问。



CN 101310285 B

1. 用于在内容分发系统中管理访问控制的方法，所述系统具有根据预定义的数据访问格式的访问控制，所述系统包括：

- 用于提供内容数据和相关元数据的至少一个组织 (32)；
- 用于呈现所述内容数据和相关元数据并且执行应用的呈现设备 (39)；以及
- 用于操纵所述内容数据和相关元数据的至少一个应用，

该方法包括以下步骤：

- 根据所述预定义的数据访问格式为所述组织设置访问策略，所述访问策略包括用于控制对所述呈现设备的资源以及对所述内容数据和相关元数据的访问的访问参数；
- 提供符合所述组织的访问策略的至少一个组织应用 (35)；
- 提供符合对应的组织的访问策略的内容数据和相关元数据，

以使得所述呈现设备能够执行所述组织应用并且同时根据所述组织的访问策略来访问所述呈现设备的资源，

其中，该方法还包括以下步骤：

- 保持用户访问策略，其在执行所述组织应用的同时相对于所述组织的访问策略限制对所述呈现设备的资源的访问；以及
- 基于附加的信任数据来调节对应于所述组织的用户访问策略，以便选择性地允许所述组织应用根据所述组织的访问策略来访问所述资源。

2. 如权利要求 1 所述的方法，其中，该方法包括：

- 在远程数据库设备处保持信任数据集合；以及
- 从该集合中获取信任数据以便调节所述用户访问策略，

在特定情况下，该方法还包括通过网络访问所述远程数据库设备。

3. 如权利要求 1 所述的方法，其中，所述附加的信任数据包括有限数目的信任级别。

4. 如权利要求 3 所述的方法，其中，所述信任级别包括：

- 完全受信级别，其允许所述组织应用根据所述组织的访问策略来完全访问所述资源；
- 部分受信级别，其允许所述组织应用访问预定义的资源子集；以及
- 不受信级别，其不允许所述组织应用访问所述资源。

5. 如权利要求 1 所述的方法，其中，所述用户访问策略包括初始地为在所述呈现设备 (39) 中所不知道的组织设置不受信级别，所述不受信级别不允许所述组织应用访问所述资源。

6. 如权利要求 1 所述的方法，其中，所述呈现设备的所述资源包括以下各项的至少其中之一：

- 网络连接；
- 用于存储数据的存储器位置；
- 系统或设备参数；
- 个人用户数据，比如名称或信用卡数据。

7. 用于在内容分发系统中管理访问控制的设备，所述系统具有根据预定义的数据访问格式的访问控制，所述系统包括：

- 用于提供内容数据和相关元数据的至少一个组织 (32)；

- 用于呈现所述内容数据和相关元数据并且执行应用的呈现设备 (39) ;以及

- 用于操纵所述内容数据和相关元数据的至少一个应用，

该设备包括 :

- 用于根据所述预定义的数据访问格式为所述组织设置访问策略的装置，所述访问策略包括用于控制对所述呈现设备的资源以及对所述内容数据和相关元数据的访问的访问参数 ;

- 用于提供符合所述组织的访问策略的至少一个组织应用 (35) 的装置 ;

- 用于提供符合对应的组织的访问策略的内容数据和相关元数据的装置，

以使得所述呈现设备能够执行所述组织应用并且同时根据所述组织的访问策略来访问所述呈现设备的资源，

其中，该设备还包括 :

- 用于保持用户访问策略的装置，其在执行所述组织应用的同时相对于所述组织的访问策略限制对所述呈现设备的资源的访问 ;以及

- 用于基于附加的信任数据来调节对应于所述组织的用户访问策略，以便选择性地允许所述组织应用根据所述组织的访问策略来访问所述资源的装置。

8. 如权利要求 7 所述的设备，其中，该设备包括 :

- 用于在远程数据库设备处保持信任数据集合的装置 ;以及

- 用于从该集合中获取信任数据以便调节所述用户访问策略的装置，

以及，在特定情况下，该设备还包括通过网络访问所述远程数据库设备的装置。

9. 如权利要求 7 所述的设备，其中，所述附加的信任数据包括有限数目的信任级别。

10. 如权利要求 9 所述的设备，其中，所述信任级别包括 :

- 完全受信级别，其允许所述组织应用根据所述组织的访问策略来完全访问所述资源 ;

- 部分受信级别，其允许所述组织应用访问预定义的资源子集 ;以及

- 不受信级别，其不允许所述组织应用访问所述资源。

11. 如权利要求 7 所述的设备，其中，所述用户访问策略包括初始地为在所述呈现设备 (39) 中所不知道的组织设置不受信级别，所述不受信级别不允许所述组织应用访问所述资源。

12. 如权利要求 7 所述的设备，其中，所述呈现设备的所述资源包括以下各项的至少其中之一 :

- 网络连接 ;

- 用于存储数据的存储器位置 ;

- 系统或设备参数 ;

- 个人用户数据，比如名称或信用卡数据。

用于管理访问控制的系统

技术领域

[0001] 本发明涉及一种用于在内容分发系统中管理访问控制的方法，所述系统具有根据预定义数据访问格式的访问控制，所述系统包括用于提供内容数据和相关元数据的至少一个组织、用于呈现所述内容数据和相关元数据并且执行应用的呈现设备以及用于操纵所述内容数据和相关元数据的至少一个应用，该方法包括以下步骤：根据所述预定义数据访问格式为所述组织设置访问策略，所述访问策略包括用于控制对所述呈现设备的资源以及对所述内容数据和相关元数据的访问的访问参数；提供符合所述组织的访问策略的至少一个组织应用；提供符合对应的组织的访问策略的内容数据和相关元数据，以使得所述呈现设备能够执行所述组织应用并且同时根据所述组织的访问策略来访问所述呈现设备的资源。

[0002] 本发明还涉及用在所述系统中的计算机程序产品和呈现设备。所述呈现设备包括：呈现装置，其用于生成媒体信号以便呈现所述数据和相关元数据；以及访问控制装置，其用于执行所述组织应用并且同时根据所述组织的访问策略来访问所述呈现设备的资源。

[0003] 本发明涉及到由诸如电影工作室之类的组织在用户设备中提供多媒体和交互式应用的领域。所述应用可以包括呈现图像、背景视频、游戏以及收集并存储观看数据和文字评论等等。通常来说，这种交互式应用基于根据预定义格式的所存储的内容数据和相关元数据。特别地，本发明涉及到控制对通常由某一组织提供及拥有的这种专有数据(proprietary data)的访问。

背景技术

[0004] 文献US2004/0148514描述了一种呈现系统，其包括存储介质以及用于在显示器上呈现所存储的交互式应用的数据（例如视频）的再现方法。诸如光盘播放器的读取设备从记录载体获取所存储的信息，所述信息例如是包括数字压缩视频数据的音频/视频(AV)流。软件出版商（或组织）可以提供所述内容数据（例如音频/视频）和相关元数据（例如重放控制数据、背景文字和图像、交互式应用等等）。该文献描述了控制对这种数据的访问以及实现根据预定义访问控制格式的策略的多种方式。例如，描述了用于保护及控制对这种数据的访问的加密方法。可以由认证权威机构发行数字证书。所述访问策略特别适于通过由对应的出版商或组织所提供的应用来控制对所述专有数据的访问。此外，所述访问策略可以控制对所述呈现设备中的资源的访问，这例如是通过许可访问本地存储容量、网络连接或者特定系统数据而实现的。

[0005] 根据所述已知系统的访问策略是基于以下假设确立的：所述应用（即所述组织）的行为良好，这是因为所述组织必须遵循所述访问控制格式。因此，所述访问控制系统针对由所述组织提供或者在对应组织的控制下分发的应用提供了对访问资源或专有数据的应用的适当控制。然而，当应用虽然是源自符合所述访问策略的所有要求的来源但是却行为欠佳时，就会出现问题。

[0006] US 6092194描述了一种用于保护计算机和网络免受恶意下载的系统和方法。该系统应用一种安全性策略，以便决定是否允许把可执行软件下载到计算机上。所述安全性策

略或者允许下载并且随后激活所述软件，或者阻止所述下载。所述安全性策略可以包括使用已知的恶意或可允许下载的列表、受信任的证书或者受信任的源 URL 的列表。所述安全性策略可以被个人化。

发明内容

[0007] 本发明的一个目的是提供一种访问控制系统，其允许在访问受控环境中对符合已建立的访问策略的应用进行进一步的控制。

[0008] 为此目的，根据本发明的第一方面，在开头段落中描述的所述方法还包括以下步骤：保持用户访问策略，其在执行所述组织应用的同时相对于所述组织的访问策略限制对所述呈现设备的资源的访问；以及基于附加的信任数据来调节对应于所述组织的用户访问策略，以便选择性地允许所述组织应用根据所述组织的访问策略来访问所述资源。

[0009] 为此目的，根据本发明的第二方面，在开头段落中描述的所述设备中，所述访问控制装置被设置成执行以下操作：保持用户访问策略，其在执行所述组织应用的同时相对于所述组织的访问策略限制对所述呈现设备的资源的访问；以及基于附加的信任数据来调节对应于所述组织的用户访问策略，以便选择性地允许所述组织应用根据所述组织的访问策略来访问所述资源。

[0010] 为呈现设备的用户创建用户访问策略。所述用户访问策略是规则和参数的集合，其进一步限制对所述用户的呈现设备的资源的访问。可以按照任何适当的方式来提供所述附加的信任数据，例如由用户主动提供、通过因特网从用户选择的外部源自动提供等等。因此，所述用户访问策略的限制被应用来影响适用于对应的组织应用的已经被接受并且已经被认证的访问策略。

[0011] 所述措施的效果在于，在所述呈现系统中，所述用户访问策略被应用来提供对已经遵循对应的组织的访问策略的组织应用的用户控制，其中所述对应的组织的访问策略符合所述访问控制格式。有利地，如果用户不想要对所述呈现设备中的资源的访问，则其有机会限制这种访问，尽管根据所述访问策略这种访问是允许的。

[0012] 本发明还基于以下认识。例如可以从上面讨论的 US2004/0148514 中获知用于控制对专有数据的访问的访问控制格式，其中所述专有数据仅仅对应于专有者或者对应于特定的以及预先定义的第三方。此外，用于分发诸如 BD 格式（蓝光光盘；可以在 http://www.blu-raydisc.com 并且特别是在 http://www.blu-raydisc.com/Section-13628/Index.html 处找到描述，同时 Section-13890 包含对应于 BD 的 Java 编程语言的规范）以及 MHP 标准（数字视频广播多媒体家用平台规范 1.0.3，ETSI TS 101812 V1.3.1-2003-06，可以从 ETSI 网站 http://www.etsi.org 获得）的多媒体内容的其他系统提供了访问控制策略的其他实例。例如，所述 MHP 标准允许针对访问文件或子目录或者针对使用可以在设备中获得的其他资源授予许可。在这些例子中，所述访问策略被以密码方式加强。

[0013] 然而，本发明的发明人已经看到，需要由用户进行进一步的控制。例如，一旦为某一组织建立了访问策略之后，如果该组织不再受到信任，该组织还可以使用许可。此外，各组织可以使用对于某些用户来说可接受但是对于其他用户来说不可接受的资源。所提供的解决方案是：建立所述用户访问策略，以便附加地控制对所述呈现设备的资源的访问。某些组织无法像其他组织那样受到信任。某些最近停业的组织的密钥可能仍然被用来放出由该

组织的通用访问控制策略所管理的内容和应用。出于很明显的原因，该内容的可信赖性是很可疑的。或者，由于用户不习惯于从某一组织购买电影，因此该用户可能就是不知道该组织。本发明的发明人已经看到，上述情况不同于因特网上的“不受信任的网站”的问题，并且无法通过由因特网浏览器提供的相同措施来解决上述情况。因特网浏览器基于类别（内联网、受信任、受限制）对站点进行分类，并且为每一类定义一个信任级别。在所述内容分发系统中，应用将等效于网站。但是无法像网站那样按照类别来对应用进行分组。本发明的发明人已经看到，可以通过对于每个来源（即每个组织）提供所述用户访问策略来控制应用。对于因特网浏览器来说可以接受的是每个站点都是可疑的并且只有经过用户准许之后才可以操作，这对于用户已购买的记录载体上的多媒体数据来说是不可接受的，所述记录载体应当简单地进行播放。有利的是，所述用户访问策略提供了针对不受信任的组织应用以及可疑的组织的保护，同时还允许呈现所分发的内容数据。

[0014] 在一个实施例中，所述方法包括在远程数据库实体处保持信任数据集合以及从该集合中获取信任数据以便调节所述用户访问策略，在特定情况下，所述方法还包括通过网络访问所述远程数据库实体。可以通过任何适当的载体来传送所述信任数据，比如通过记录载体或者通过所述网络。因此，运行所述数据库实体的另一方有效地设置所述信任数据，所述信任数据被应用在所述呈现设备中以便设置所述用户访问策略。这样做的优点在于，用户可以在之前选择这种远程数据库实体以便根据所述用户的优选项保持最新的信任数据集合。随后基于所述获取的信任数据来自动设置所述用户访问策略。

[0015] 在所述方法的一个实施例中，所述用户访问策略包括初始地为在所述呈现设备中未知的组织设置不受信级别，所述不受信级别不允许所述组织应用访问所述资源。这样做的优点在于，未知源的应用不能访问资源，除非用户通过设置用户访问策略而肯定地许可所述访问。

[0016] 在所附权利要求书中给出了根据本发明的设备和方法的其他优选实施例，其公开内容被合并在此以作参考。

附图说明

[0017] 通过参照在下面以举例的方式描述的实施例以及参照附图，本发明的这些和其他方面将变得显而易见，其中：

[0018] 图 1 示出了存储介质；

[0019] 图 2 示出了呈现设备；

[0020] 图 3 示出了具有根据预定义的数据访问格式的访问控制的内容分发系统；以及

[0021] 图 4 示出了文件访问控制机制。

[0022] 不同附图中的相应元件具有完全相同的附图标记。

具体实施方式

[0023] 图 1 示出了盘状记录载体 11，其具有轨道 9 和中心孔 10。所述轨道 9 是表示信息的一系列已记录（将被记录）的标记的位置，其被设置成螺旋匝图案，从而在信息层上构成基本上平行的轨道。所述记录载体可以是光学可读的，其被称作光盘。光盘的例子有 CD 和 DVD 以及使用蓝色激光的高密度光盘（其被称作蓝光盘 (BD)）。可以在以下参考文献中找

到关于DVD盘的进一步的细节：ECMA-267：120mmDVD-Read-Only Disc-(1997)。通过沿着所述轨道的光学可检测的标记在所述信息层上表示所述信息。

[0024] 所述记录载体11用于在文件管理系统的控制下成块地携带数字信息。所述信息包括将被连续再现的实时信息，特别是表示数字编码的视频（比如MPEG2或MPEG4）的信息。

[0025] 在新的光盘标准中，可以把高清晰度视频与各种图形和应用相组合以便产生交互式观看体验，例如可以把视频与交互式应用相组合，以便增强观看体验。一般来说，这些应用允许用户控制对视频内容的重放、获得关于正在观看的内容的更多信息或者访问新的服务。对于新的服务来说，用户设备可以具有通信接口，以便建立到诸如因特网之类的网络的连接。通过该连接，所述应用例如可以在诸如电视(TV)的显示设备上提供电子商务服务、赌博服务和信息服务。此外，可以在每个记录介质的播放器中获得诸如硬盘驱动器(HDD)之类的非易失性存储介质，以便例如存储所下载的信息。

[0026] 所述存储介质根据预定义的数据存储格式携带内容信息和相关元数据，例如视频和相关数据（其中包括诸如按钮、图形单元或动画之类的虚拟对象）、关于所述内容信息的背景信息、附加的游戏或交互式工具等等。所述内容数据和相关元数据由所谓的组织（即内容提供商和/或所有者）提供。对于所述组织来说，所述数据被称作“专有的”意味着所述数据在对应的组织的控制之下和/或属于该对应的组织所有。所述预定义的数据存储格式允许对例如HDD上的数据以及诸如通信接口之类的服务进行访问控制（例如通过使用密码方法），从而仅仅能够根据适用的版权规定来使用。根据预定义的数据访问格式为特定组织创建的规则和参数的集合被称作访问策略。

[0027] 图2示出了用于再现实时信息和有效信息的呈现设备。该设备具有读取装置和扫描装置，所述读取装置包括用于获取所存储的信息的光头22，所述扫描装置用于扫描上述记录载体11的轨道。该扫描装置包括用于旋转记录载体11的驱动单元21、用于在径向方向上把光头22粗糙定位在所述轨道上的定位单元25以及控制单元20。光头22包括已知类型的光学系统，其用于生成辐射光束24，所述辐射光束被引导通过各光学元件从而聚焦到所述记录载体的信息层的轨道上的辐射点23处。辐射光束24由例如激光二极管的辐射源生成。所述光头还包括（未示出）聚焦致动器和寻轨致动器，所述聚焦致动器用于沿着所述光束的光轴移动辐射光束24的焦点，所述寻轨致动器用于在径向方向上把所述辐射点23精细定位在轨道的中心处。

[0028] 所述控制单元20通过控制线26（例如系统总线）连接到将被控制的其他单元。该控制单元包括例如微处理器的控制电路、程序存储器和控制门，以便如下所述地执行根据本发明的程序和功能。还可以用逻辑电路把控制单元20实现为状态机。

[0029] 为了进行读取，在光头22中利用通常类型的检测器（例如四象限二极管）来检测由所述信息层反射的辐射，以便生成读取信号和其他检测器信号，其中包括用于控制所述寻轨和聚焦致动器的寻轨误差信号和聚焦误差信号。所述读取信号由呈现单元30处理，以便呈现所存储的信息并且生成显示信号，从而在诸如监视器或电视机之类的显示器上显示所存储的信息以及访问所存储的信息中的虚拟对象。所述显示包括显示及执行所述虚拟对象，比如在交互式用户接口中调用命令的按钮或者在再现实时信息期间的动画。

[0030] 根据本发明，所述设备具有访问控制单元31，其用于执行应用并且同时根据所述

组织的访问策略来访问所述呈现设备的资源 41。所述资源 41 包括可能受到应用影响或者由其使用的所述呈现设备的任何特征，并且可以包括以下各项：网络连接，比如用于连接到因特网的调制解调器；本地存储装置，比如用于存储应用数据的硬盘或固态存储器；各种系统参数或设备参数，比如家长控制设置或声级；或者个人用户数据，比如用户名、家庭数据或信用卡数据。

[0031] 所述应用是通常由某一组织通过软件提供的可以在所述呈现设备上获得的功能。所述应用还可以由不同的来源提供，比如所述呈现设备的制造商或者来自独立软件公司的一般类型的应用。根据本发明的访问控制单元 31 的具体功能是：保持用户访问策略，其相对于所述组织的访问策略针对所述组织应用初始地限制对所述呈现设备的资源 41 的访问；以及基于附加的信任数据来调节对应于所述组织的用户访问策略，以便选择性地允许所述组织应用根据所述组织的访问策略来访问所述资源。下面将参照图 3 进一步阐述。

[0032] 应当注意到，所述应用、部分应用或者相关功能可以被实现为所述访问控制单元中的驻留功能。或者，可以通过其他信息载体或者通过网络（比如因特网）把所述应用提供在所述记录载体上。所述访问控制单元 31 可以被实现为所述控制单元 20 中的软件功能、实现为所述呈现单元 30 的一部分或者实现为单独的单元。

[0033] 所述设备可以被设置成在某种类型的记录载体 11 上写入信息，所述记录载体是可写的或者可重写的，比如 DVD+RW 或者 BD-RE。于是所述设备包括写入单元 29，其用于处理输入信息以便生成用来驱动所述光头 22 的写入信号。

[0034] 在所述呈现系统的一个实施例中，所述呈现设备可以从远程源获取内容数据和相关元数据。在用户位置处的所述呈现设备可以通过网络连接到服务器。所述用户设备（例如机顶盒 (STB)）具有用于接收诸如视频的广播数据的接收器。该用户设备具有诸如调制解调器的网络接口，以便把该设备连接到诸如因特网的网络。服务器也具有网络接口，以便把该服务器设备连接到所述网络。应当注意到，可以连接到网络的所述用户设备还包括多媒体设备（例如标准化的多媒体家用平台 MHP）、增强的移动电话、个人数字助理等等。

[0035] 图 3 示出了具有根据预定义的数据访问格式的访问控制的内容分发系统。该系统 300 具有用于提供第一内容数据和相关元数据的第一组织 32 以及用于提供第二内容数据和相关元数据的第二组织 33。为了分发内容，所述系统还具有用于携带第一专有数据的第一记录载体 34 以及用于携带第二专有数据的第二记录载体 36。或者，可以通过不同的渠道来分发所述专有数据或其一部分（比如相关元数据），所述渠道比如是因特网之类的网络。第一组织 32 还可以提供用于操纵所述第一内容数据和相关元数据的至少一个组织应用 35。第二组织 33 还可以提供用于操纵相应的第二数据的至少一个组织应用 37。

[0036] 呈现设备 39 被提供来从记录载体呈现所述内容数据和相关元数据，正如箭头 34’、36’ 和 38’ 所指示的那样。所述呈现设备可以被耦合到显示器 40 以及通过网络接口耦合到网络 43。在一个实施例中，呈现设备 39 通过网络 43 接收所述内容数据和 / 或相关元数据。还可以有效地在所述呈现设备中执行所述应用。所述应用最初可以被包括在所述呈现设备中，或者可以例如通过所述网络单独分发所述应用并且将其存储在所述呈现设备中。应当注意到，所述记录载体用于携带所述内容数据和相关元数据，但是还可以携带所述应用。

[0037] 每个组织具有对应的访问策略，即根据预定义的访问控制格式的参数和规则的集

合。第一组织应用 35 能够根据第一访问策略访问第一专有数据，第二组织应用 37 能够访问第二专有数据。对应于某一应用的访问策略部分地由所述系统设置（例如应用 35 无法访问与应用 37 相关联的“本地”存储装置上的数据），并且部分地由所述组织本身设置（例如组织 32 允许组织 33 的应用 37 访问与应用 34 相关联的数据）。仅仅得到许可的组织具有用来产生后一种策略的密码密钥。

[0038] 应当注意到，可以通过分别具有对应的专有数据的其他组织和相应的其他记录载体 38 和 / 或应用来扩展所述系统，同时每一个组织通常将具有多组专有数据（例如电影制作和针对用户的相应的额外内容），同时在多个记录载体上商务地叠加每一组（制作）。

[0039] 所述访问控制单元 31 被附加地安排成例如基于通过用户接口得到的用户输入来设置用户访问策略。所述用户访问策略限制对所述呈现设备的资源 41 的访问。应当注意到，所述组织的访问策略主要被加强来控制对所述资源的访问，正如在所述数据访问格式中所定义的那样。所述用户访问策略还根据用户的优选项来影响及限制所述访问。

[0040] 用户可以明确地把所述优选项设置到所期望的值，或者可以根据来自外部源的信任数据来设置或调节这种设置。例如，所述呈现设备的制造商可以把初始优选项设置在安全且受限的级别，这随后可以被用户改变。因此，所述访问控制单元被设置成基于附加的信任数据来调节所述用户访问策略，从而选择性地允许所述组织应用在根据所述组织的访问策略所确定的最大允许访问级别下访问所述资源。

[0041] 在一个实施例中，所述内容分发系统 300 包括远程数据库实体 42，其用于保持信任数据的集合。所述远程数据库实体可以经由用于连接到网络的网络接口 44 通过诸如因特网的网络 43 耦合到所述呈现设备。所述数据库实体 42 具有用于存储数据的数据库单元 45，该单元被设置成保持信任数据的集合。所述保持尤其可以包括针对行为欠佳的组织调整所述信任数据、针对新组织添加新的信任数据、针对特定组织使用用户反馈等等。在所述呈现设备的请求下或者自动地或周期性地，所述数据库实体把所述信任数据的所需子集从所述集合通过网络接口装置 44 传送到所述呈现设备。随后，所述呈现设备基于所述信任数据针对所述组织调节所述用户访问策略，以便选择性地允许所述组织应用根据所述组织的访问策略来访问所述资源。例如，所述远程数据库实体可以由所述呈现设备的制造商提供、由消费者组织提供、由隐私意识团体提供等等。所述访问控制单元 31 被设置成从所述信任数据集合中获取信任数据以便调节所述用户访问策略。

[0042] 在一个实施例中，所述附加信任数据包括有限数目的信任级别，例如仅仅包括两个信任级别 :完全受信或者根本不受信。如果设置了第一级别，则所述组织应用可以根据所述组织的访问策略的设置对所述资源进行完全访问。如果设置了第二级别，则所述组织应用根本无法访问所述资源，尽管所述组织的访问策略的设置允许进行这种访问。

[0043] 在另一个实施例中，所述信任级别包括三个级别 :完全受信级别，其允许所述组织应用根据所述组织的访问策略来完全访问所述资源 ;部分受信级别，其允许所述组织应用访问预定义的资源子集 ;以及不受信级别，其不允许所述组织应用访问所述资源。此外，所述访问控制单元 31 可以被安排成设置在所述部分受信级别中所允许的特定访问，例如允许访问商店数据，但是不允许访问访问信用卡数据。

[0044] 在一个实施例中，所述用户访问策略包括 :对于在所述呈现设备 39 中所不知道的组织初始地设置不受信级别。所述不受信级别不允许所述组织应用访问所述资源。所述访

问控制单元 31 被设置成对于来自新的未知组织的任何应用阻断其访问。

[0045] 图 4 示出了文件访问控制机制。该图示意性地示出了文件系统 60，其具有根目录 61 和对应于多个组织的各组织子目录 62。每个组织可以具有对应于多部电影的另外的电影子目录 63。在每个目录中可以存在文件，例如，在子目录 63 “电影 1a”中存在音频视频文件 69 和被称作“Xlet1a”的应用文件 64，并且在其他子目录中存在被称作“Xlet1b”的应用 70 和被称作“Xlet3a”的应用 71。每个子目录或文件具有许可指示符 66，例如“UNIX 许可”，其指示对应于访问该子目录的不同用户的进行读写的权利。根据所述数据访问格式，每个应用可以具有凭证 65 并且可以包含访问参数以便访问专有信息，其中所述凭证是指示所述访问权利的附加数据量（通常是在单独的文件中）。应当注意，应用 70(Xlet1b) 可以对文件 69(A/V2，其具有组读访问）进行读访问，但是如箭头 68 所示，其不被允许启动应用 64(Xlet1a，其仅仅具有电影所有者访问）。应用 71(Xlet3a) 不处在与应用 64(Xlet1a) 和文件 69(A/V2) 相同的组（组织 1) 中，因此其需要例如由组织 1 签过名的特殊凭证 65，以便如箭头 67 所示访问文件 64(A/V2)。

[0046] 如图 4 中所示的数据访问格式的一个实施例是基于 Java，并且可以被使用在蓝光盘 ROM 全特征模式下。这种 BD-ROM 播放器包括 Java 虚拟机 (JVM)，其可以运行小的应用（通常被称作 Xlet 的程序）。这些灵活且强大的呈现机还具有网络连接，并且可以具有硬盘驱动器 (HDD) 形式的本地存储装置。所述内容所有者（即组织）可以在所述 BD-ROM 盘上与电影一起分发所述应用，或者可以通过网络连接来分发。在对这种系统的标准访问控制中，仅有在受保护的存储器位置处（也被称作钥匙箱的设备资源）存储任何访问参数的原始应用可以取回所述访问参数。

[0047] 根据 MHP（参考上面的内容）的数据访问格式是 Java 的子集和扩展，以便允许在机顶盒 (STB) 上运行 Java Xlet，从而进行浏览、与 A/V 数据进行交互等等。当加载一个应用时，首先由所述系统对其进行认证。该系统随后把所述应用作为该系统（类似于 Unix 操作系统）上的一个用户来对待（基于“应用 id”），其具有归属目录、其所属于的组（“组织 id”）。根据所述访问策略（其被称作许可请求文件），所述应用与访问参数一起到来，通过所述访问参数该应用从所述系统请求某些资源（网络访问等等），可以根据所述访问策略文件来准许所述请求。

[0048] 所述数据访问格式随后使用这些特征对存储在所述呈现设备的本地存储装置上的数据定义一个两层访问结构：

[0049] 1、Unix 风格的许可权利：（或者默认策略）数据被作为文件存储在普通的目录树中。对于以下每个级别，每个文件和目录被赋予读 / 写访问许可 66（参见 MHP，第 12.6.2.7.2 节）：

[0050] a、应用（创建所述数据的应用）

[0051] b、组织（属于与所述创建应用相同的组织的应用）

[0052] c、世界（所有应用）

[0053] 2、凭证机制：为了推翻上面的机制并且提供更加细粒度的访问，（多个）文件 / 目录的所有者可以准备凭证 65，其是（签过名）的声明，其表明（例如来自另一组的）其他应用可以访问所述（多个）文件 / 目录。凭证 65 被包含在上面提到的许可请求文件中。在加载了所述应用之后，所述系统可以基于所述凭证和所述策略文件决定该应用应当可以访

问附加文件（参见 MHP，第 12.6.2.6 节）。上面的目录 / 文件访问控制机制可以被用于诸如 BD-ROM 之类的记录载体。在这种情况下，“应用 id”对应于与特定盘相关联的应用，“组织 id”对应于组织。

[0054] 为了增强所述访问控制机制，可以如上所述地创建所述用户访问策略。下面描述另一个例子。诸如蓝光盘 (BD) 之类的新的内容分发系统支持 Java 代码，以便允许交互式应用。Java 得到支持的方式大体上与 GEM（全局可执行 MHP，参见 MHP 参考文献）相符，其中包括安全性部分。结果，BD 的安全性模型通过对受信任的应用进行签名来保护用户不受恶意代码的损害。各组织认证其所提供的应用是适当的。这是通过直接对其签名或者通过认证所述软件的生产商（其对所述软件签名）是合法的而实现的。认证权威机构 (CA) 随后认证所述组织凭证是有效的（参见以下内容）。

[0055] 所述用户访问策略允许用户在应用所述安全性策略时在各组织之间进行区分。对应于不同组织的单独的用户访问策略（其是基于组织标识符而选择的，比如组织 ID）对于来自受信任的组织的应用允许对资源的不受限制的使用，对于来自未知组织的应用允许对资源的在某种程度上受限制的使用，并且对于来自明确地不受信任的组织的应用只允许对资源的非常受限制的使用。应当注意到，在后一种情况下，签过名的（因此是经过认证的）应用（换句话说是应当可以根据所述数据访问格式获得完全访问的应用）将不会获得完全访问，这是因为用户不信任其来源。所述用户访问策略实质上将这种应用恢复到未经认证的应用。

[0056] 通过为每个组织分配一个信任级别，所述用户访问策略自动为新的应用分配适当的信任级别，其前提是该新的应用是来自已经为之设置了用户策略的组织。通过为任何新的组织分配最低的信任级别，为所有组织设置了用户策略。用户将有机会升级对应于某一组织的信任级别，从而对于该组织的所有应用自动升级。这样，用户在管理信任级别过程中的工作量非常有限。有利的是，使得用户更加方便的上述做法绝不会损害所述平台的安全性。

[0057] 对于每个组织都存在某些分类选项。在一个实施例中，创建了支持对组织进行分类的网站。所述网站保持对应于大量组织的信任数据的列表。在所述列表上将标识出任何可疑的组织，并且也将标识出任何受信任的组织。因此，可以通过经由因特网与上述网站进行联系而使得所述呈现设备中的所述分类处理完全自动化，而不会损害安全性。

[0058] 应当注意到，不意图屏蔽来自可疑组织的盘，而仅仅是限制对某些关键资源（比如信用卡号或者网络连接）的使用。根据所述组织的分类，来自特定组织的特定应用将具有指定的访问级别。

[0059] 数据访问格式可以包括以下内容。对将被认证的应用进行散列，并且通过利用所述组织的私有密钥对其进行加密来为主散列文件的散列签名。所述签名被放到盘上。相关联的公共密钥被包含在组织证书中，所述证书也被放在盘上。通过播放器具有其公共密钥的认证权威机构 (CA) 来为所述组织证书的散列签名。该签名也被放在盘上。这可以被如下表示：

[0060] $Signature_{application} = \{hash(hash(application\_code))\}_{key\_private\_organization}$

[0061] $Certificate_{organization} \approx (key\_public\_organization)$

[0062] $Signature_{organization\_certificate} = \{hash(Certificate_{organization})\}_{key\_private\_CA}$

[0063] 为了认证某一组织应用中的 Java 代码，所述呈现设备使用所述 CA 的公共密钥来验证所述组织证书的签名。如果该检查通过，则使用来自所述组织证书的所述组织的公共密钥来验证所述应用的签名。

[0064] 可能还有另一个信任级别，在该信任级别下，所述 Java 代码的生产商使用其自身的密钥集合来认证所述应用。在这种情况下，所述组织需要为所述生产商的证书签名。这可以被如下表示：

[0065] $Signature_{application} = \{hash(hash(application\_code))\}_{key\_private\_producer}$

[0066] $Certificate_{producer} \approx (key\_public\_producer)$

[0067] $Signature_{producer\_certificate} = \{hash(Certificate_{producer})\}_{key\_private\_organization}$

[0068] $Certificate_{organization} \approx (key\_public\_organization)$

[0069] $Signature_{organization\_certificate} = \{hash(Certificate_{organization})\}_{key\_private\_CA}$

[0070] 应当注意到，如上所述地提供所述用户访问策略功能的访问控制单元 31 可以由用于在用户设备中执行的计算机程序产品来提供。所述程序适于使得标准用户设备（例如膝上型计算机）的处理器执行保持及调节所述用户访问策略的各步骤。例如可以通过因特网或者在记录载体上作为软件插件来分发所述程序，或者可以通过广播与任何其他应用和音频 / 视频内容一起来发送所述程序。当被加载时，所述软件控制所述应用，从而所述应用根据所述用户访问策略来访问所述设备的资源。

[0071] 虽然主要通过基于光盘的实施例解释了本发明，但是也可以应用用来分发所述内容和 / 或元数据的其他存储介质或分发系统。然而，应当注意到，本发明特别涉及到关于由某一组织提供在用户的呈现设备上的数据的安全性策略。可以为每个组织给出一定量的本地存储，以便存储与该组织相关的数据，并且可以为所述组织给出对资源的进一步访问。针对该数据的访问策略是，仅有被验证为来自该组织的应用可以访问该数据。例如，可以通过使用 Java 语言来授予许可。应用可以具有许可请求文件，把该许可请求文件与所述访问策略的各参数文件进行比较。之前，如果可疑的或者未知的组织具有根据现有的认证权威机构 (CA) 而有效的证书，则用户不可能阻止所述组织获得对系统资源的完全访问。利用本发明，如果所请求的许可被所述访问策略所允许，那么只有在所述用户访问策略也允许这种访问时才把对应的资源释放给所述应用。

[0072] 应当注意到，在本文献中，“包括”一词不排除未列出的其他元件或步骤的存在，元件之前的“一个”不排除多个这种元件的存在，任何附图标记都不限制权利要求的范围，可以通过硬件和软件来实现本发明，并且可以用同一硬件项来表示几个“装置”。此外，本发明的范围不限于所述实施例，而在于上面描述的每一个新颖特征或特征组合。

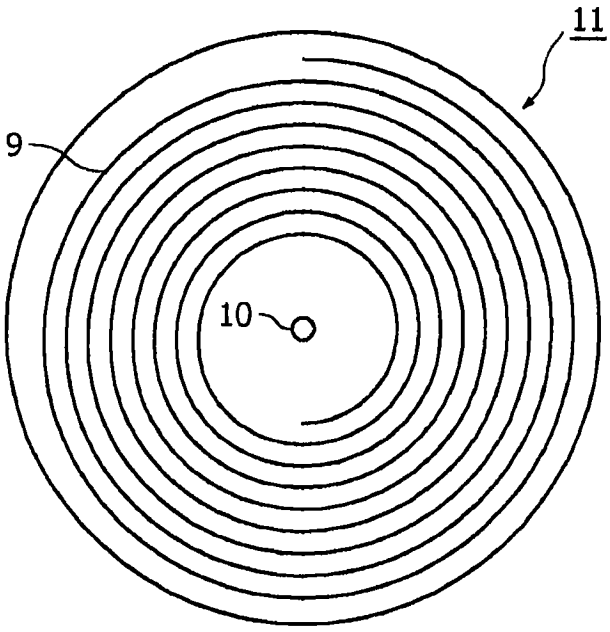


图 1

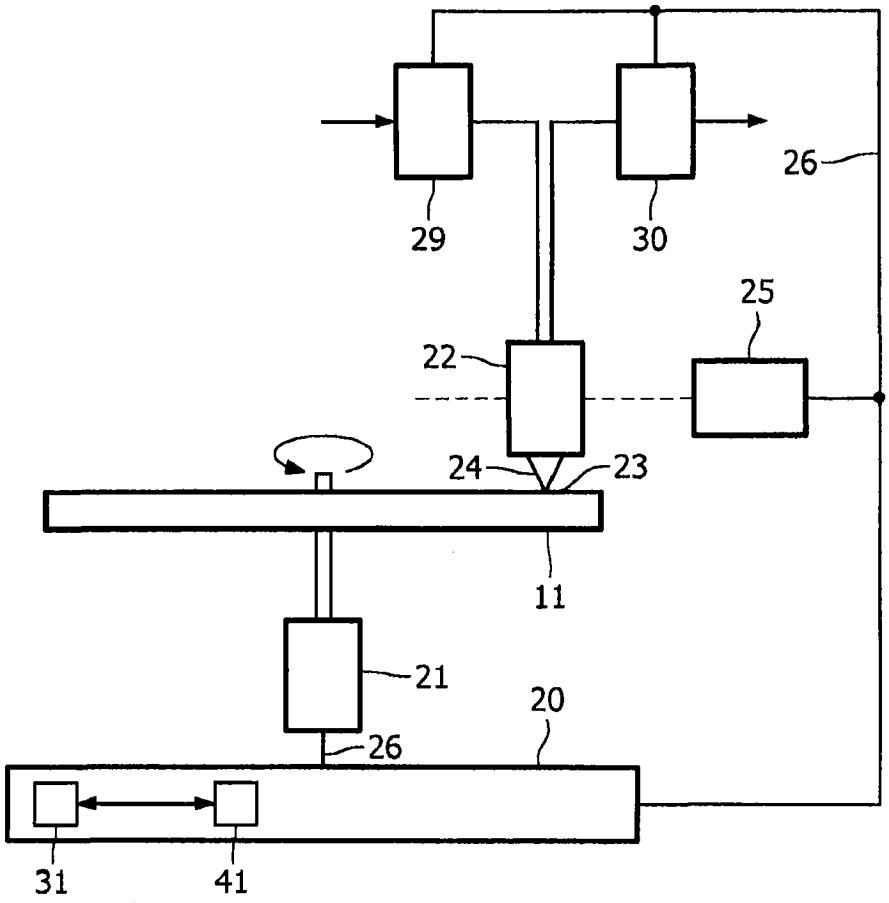


图 2

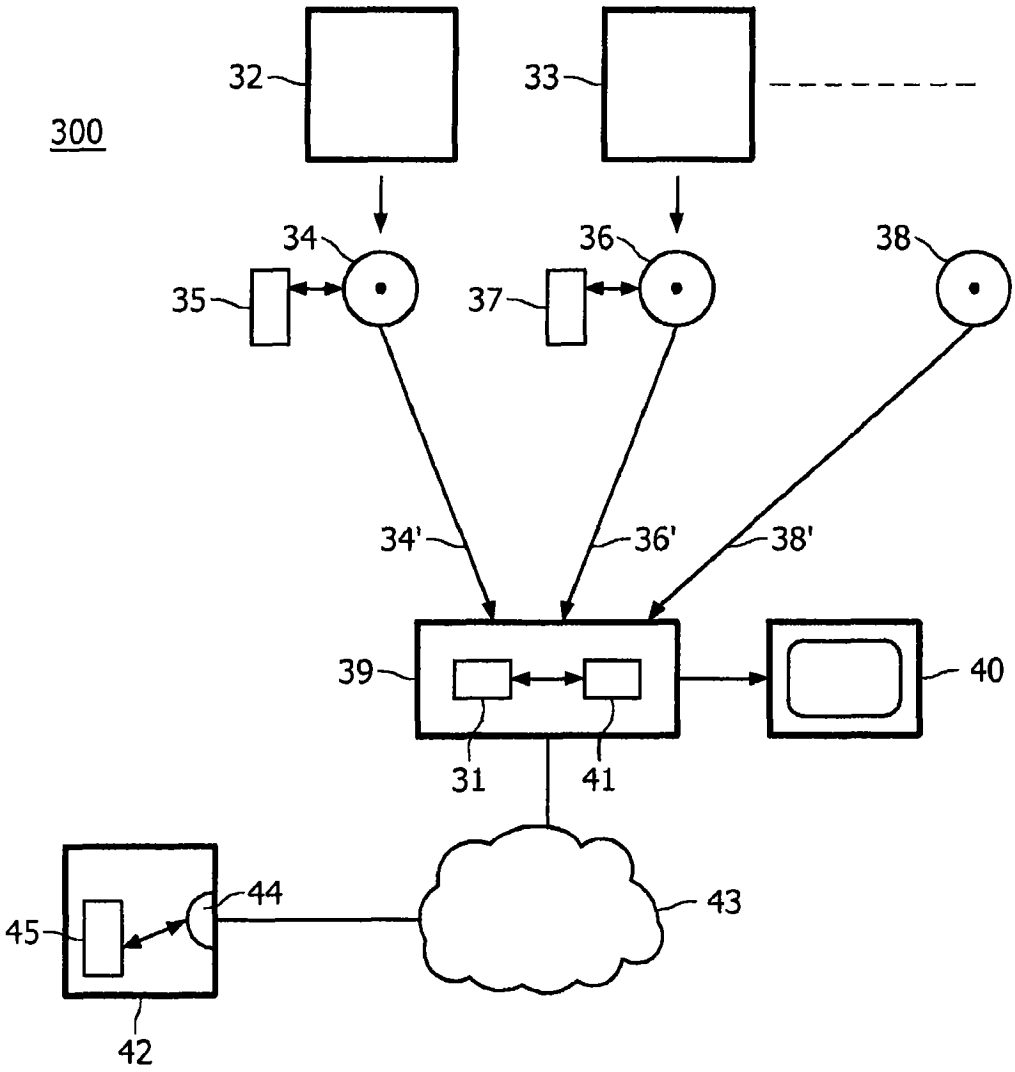


图 3

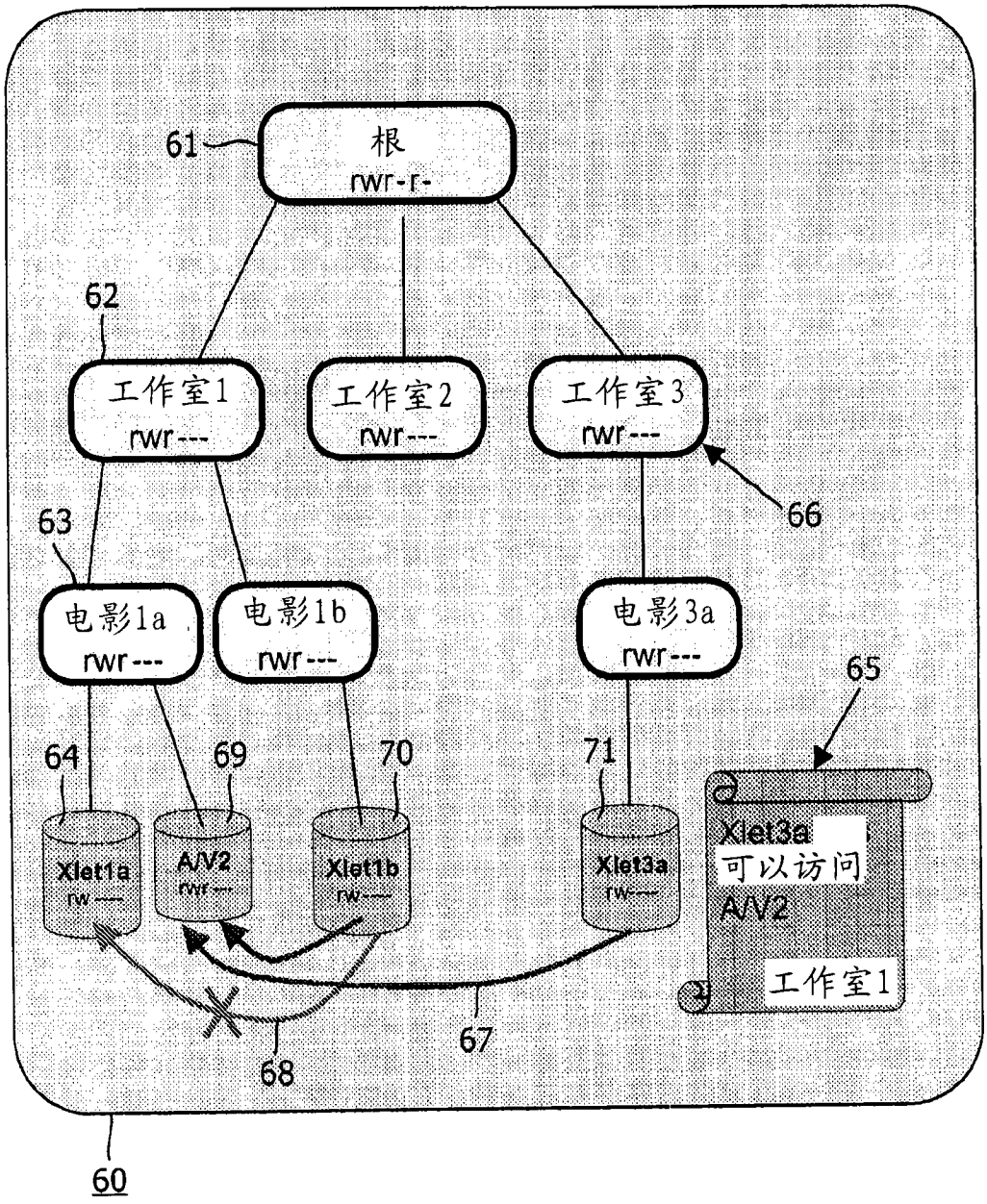

61
根
rwr-r-
62
工作室1
rwr---
工作室2
rwr---
工作室3
rwr---
66
63
电影1a
rwr---
电影1b
rwr---
电影3a
rwr---
65
64
69
70
71
Xlet1a
rw---
A/V2
rwr---
Xlet1b
rw---
Xlet3a
rw---
Xlet3a
可以访问
A/V2
工作室1
67
68
60

图 4