(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102647429 A
(43)申请公布日 2012.08.22

(21)申请号 201210134095.7

(22)申请日 2012.04.28

(71)申请人 杭州格畅科技有限公司
地址 310000 浙江省杭州市西湖区世贸丽晶城欧美中心 2 号楼(F 区)1811 室

(72)发明人 徐军 薛珂

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/56(2006.01)

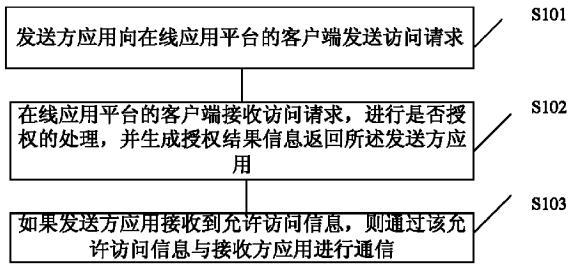
权利要求书 2 页 说明书 4 页 附图 1 页

(54)发明名称

应用间通信的访问控制方法、应用进程管理器、在线应用平台

(57)摘要

本发明的在线应用平台上应用间通信的访问控制方法、应用进程管理器，当发送方应用对接收方应用进行访问时，在线应用平台的客户端接收发送方应用的访问请求，进行是否授权的处理，并生成授权结果信息返回所述发送方应用；所述授权结果信息包括允许访问信息和拒绝访问信息。本发明的在线应用平台，包括多个应用和上述的应用进程管理器。由于本发明通过在线应用平台对应用的访问控制进行统一处理，使用本发明时用户名和密码不会多次输入，因此根本上避免了泄露问题；进行访问控制的过程中不需要进行浏览器的跳转；可支持同时调用多个应用的 API；应用提供方和调用方均无须提供额外功能以支持方案的访问控制。



CN 102647429 A

1. 一种在线应用平台上应用间通信的访问控制方法，其特征在于，包括步骤：

当发送方应用对接收方应用进行访问时，在线应用平台的客户端接收发送方应用的访问请求，进行是否授权的处理，并生成授权结果信息返回所述发送方应用；所述授权结果信息包括允许访问信息和拒绝访问信息。

2. 根据权利要求 1 所述的访问控制方法，其特征在于，所述在线应用平台的客户端进行是否授权的处理的过程包括步骤：

在预先存储的可授权应用列表中查找所述发送方应用，如果找到，则生成所述允许访问信息。

3. 根据权利要求 2 所述的访问控制方法，其特征在于，所述在线应用平台的客户端进行是否授权的处理的过程还包括步骤：

如果在预先存储的不可授权应用列表中找到所述发送方应用，则生成拒绝访问信息；如果未找到，则提示用户是否对所述发送方应用授权，并根据用户的返回结果将所述发送方应用加入所述可授权应用列表或不可授权应用列表，并生成所述授权结果信息。

4. 根据权利要求 1 所述的访问控制方法，其特征在于，所述在线应用平台的客户端进行是否授权的处理的过程包括步骤：

在预先存储的 ACL 表中查找所述发送方应用的服务，如果找到，则生成所述允许访问信息，所述 ACL 表为访问控制列表，用于存储对所述应用的服务的访问权限。

5. 根据权利要求 1 至 5 中任一项所述的访问控制方法，其特征在于，所述在线应用平台的客户端接收发送方应用的访问请求之前还包括步骤：

当启动应用时，所述应用包括发送方应用或接收方应用，在线应用平台的客户端按照预定的通信协议创建应用进程；并记录所述应用可处理的消息类型；所述应用进程为所述应用在所述客户端运行时的存在形态，包括应用进程 ID、应用名称、上下文空间、消息队列、可执行程序路径；所述消息队列为在线应用平台与所述应用进程进行通信的载体；所述在线应用平台的客户端的授权结果信息通过所述发送方应用所对应的消息队列发送至所述发送方应用；

所述在线应用平台的客户端发送所述授权结果信息后还包括步骤：

如果所述授权结果信息为允许访问信息，则接收所述发送方应用构造的消息，所述消息包括根据预定通信协议定义的应用名称、消息类型、消息体；

将所述消息投递至接收方应用所对应的应用进程的消息队列中，以便所述接收方应用的应用进程监控消息队列中的消息，并进行处理；

当所述发送方应用或接收方应用退出时，所述在线平台的客户端销毁所述应用进程。

6. 一种在线应用平台的应用进程管理器，用于实现在线应用平台内应用间的通信，其特征在于，所述应用进程管理器位于在线应用平台的客户端，包括：

发送进程消息接口，用于收发信息，所述信息包括发送方应用的访问请求以及授权结果信息，所述授权结果信息包括允许访问信息和拒绝访问信息；

访问控制装置，用于对所述访问请求进行是否授权的处理，生成授权结果信息。

7. 根据权利要求 6 所述的应用进程管理器，其特征在于，所述应用进程管理器还包括第一存储装置，用于存储可授权应用列表；第二存储装置，用于存储不可授权应用列表；

所述访问控制装置在所述可授权应用列表中查找所述发送方应用，如果找到，则生成

允许访问信息；如果在所述第二存储装置中找到所述发送方应用，则生成拒绝访问信息；如果未找到，则提示用户是否对所述发送方应用授权，并根据用户的返回结果生成授权结果信息以及将所述发送方应用加入所述第一存储装置或第二存储装置。

8. 根据权利要求 6 所述的应用进程管理器，其特征在于，所述应用进程管理器还包括第三存储装置，用于存储 ACL 表，所述 ACL 表为访问控制列表，用于存储请求方应用标识、接收方应用标识、服务名、访问权限；

所述访问控制装置在预先存储的 ACL 表中查找所述发送方应用的服务，如果找到，则生成所述允许访问信息。

9. 根据权利要求 6 至 8 中任一项所述的应用进程管理器，其特征在于，所述应用进程管理器还包括：

进程创建接口，用于当启动应用时，所述应用包括发送方应用或接收方应用，按照预定的通信协议创建应用进程；并记录所述应用可处理的消息类型；所述应用进程为所述应用在所述客户端运行时的存在形态，包括应用进程 ID、应用名称、上下文空间、消息队列、可执行程序路径；所述消息队列为在线应用平台与所述应用进程进行通信的载体；

所述发送进程消息接口将所述信息通过发送方应用所对应的消息队列发送至接收方应用，所述消息包括根据预定通信协议定义的应用名称、消息类型、消息体；

进程销毁接口，用于当所述发送方或接收方应用退出时销毁所述发送方或接收方应用的应用进程。

10. 一种在线应用平台，其特征在于，包括多个应用和权利要求 6 至权利要求 9 中任一项所述的应用进程管理器。

应用间通信的访问控制方法、应用进程管理器、在线应用平台

技术领域

[0001] 本发明涉及在线应用平台技术，尤其涉及在线应用平台上应用间通信的访问控制方法、应用进程管理器及在线应用平台。

背景技术

[0002] 传统的应用间通信时的访问控制技术有以下几种：

[0003] 方案 1：基于用户名和密码机制

[0004] 当某应用需要代表用户使用另一应用提供的服务时，要求用户提供其在目标应用的用户名及密码，把用户名和密码作为请求的一部分投递到目标应用。目标应用验证用户名及密码，以决定是否提供服务给调用方。

[0005] 方案 2：基于 OAUTH 机制

[0006] 当某应用需要代表用户使用另一应用提供的服务时，首先会跳转到目标应用网站，用户在目标应用网站输入用户名及密码，目标网站验证通过后，会列举出本次请求访问的 API 信息，用户确认后，目标网站生成 TOKEN 并跳转回调用方网站。调用方下次使用 TOKEN 直接访问有权限的服务。

[0007] 上述方案 1 会直接泄露其它应用的用户名和密码，存在极大的安全隐患。方案 2 要求浏览器的多次跳转，用户体验极差，而且处理不了同时调用多个不同应用 API 的需求。

发明内容

[0008] 本发明提供一种在线应用平台上应用间通信的访问控制方法、应用进程管理器及在线应用平台，能否解决应用间访问控制时安全隐患问题，并提高用户体验。

[0009] 本发明的在线应用平台上应用间通信的访问控制方法，包括步骤：

[0010] 当发送方应用对接收方应用进行访问时，在线应用平台的客户端接收发送方应用的访问请求，进行是否授权的处理，并生成授权结果信息返回所述发送方应用；所述授权结果信息包括允许访问信息和拒绝访问信息。

[0011] 本发明的在线应用平台的应用进程管理器，用于实现在线应用平台内应用间的通信，所述应用进程管理器位于在线应用平台的客户端，包括：

[0012] 发送进程消息接口，用于收发信息，所述信息包括发送方应用的访问请求以及授权结果信息，所述授权结果信息包括允许访问信息和拒绝访问信息；

[0013] 访问控制装置，用于对所述访问请求进行是否授权的处理，生成授权结果信息。

[0014] 本发明的在线应用平台，包括多个应用和上述的应用进程管理器。

[0015] 由于本发明通过在线应用平台对应用的访问控制进行统一处理，使用本发明时用户名和密码不会多次输入，因此根本上避免了泄露问题；进行访问控制的过程中不需要进行浏览器的跳转；可支持同时调用多个应用的 API；应用提供方和调用方均无须提供额外功能以支持方案的访问控制。

附图说明

[0016] 图 1 为在线应用平台上应用间通信的访问控制方法流程图；

[0017] 图 2 为一个实施例中应用进程管理器的原理框图。

具体实施方式

[0018] 本发明提供的在线应用平台上应用间通信的访问控制方法，通过在线应用平台对应用进行访问控制，过程如图 1 所示：

[0019] 当发送方应用对接收方应用进行访问时，发送方应用向在线应用平台的客户端发送访问请求 (S101)，要求在线应用平台的客户端授权该发送应用与接收方应用进行通信；在线应用平台的客户端接收发送方应用的访问请求，进行是否授权的处理，并生成授权结果信息返回所述发送方应用 (S102)；所述授权结果信息包括允许访问信息和拒绝访问信息；如果发送方应用接收到允许访问信息，则接下来就通过该允许访问信息与接收方应用进行通信 (S103)，如果发送方应用收到的是拒绝访问信息，则无权与接收方进行通信。

[0020] 作为一个实施例，可以预先协商好可以授权的应用名单，并存储在可授权应用列表中，在执行步骤 S102 时，在预先存储的可授权应用列表中查找所述发送方应用，如果找到，则生成所述允许访问信息。

[0021] 另外，作为一个实施例，还可以预先协商好不可授权的应用名单，并存储在不可授权应用列表中，在执行步骤 S102 时，如果在预先存储的不可授权应用列表中找到所述发送方应用，则生成拒绝访问信息。

[0022] 值得指出的是，预先保存授权应用列表或不可授权应用列表中的一种还是同时保存两种列表可以由用户根据自己的需求确定。作为一种优选实施例，如果在所保存的列表中未找到，则提示用户是否对发送方应用授权，并根据用户的返回结果将所述发送方应用加入已保存的所述可授权应用列表或不可授权应用列表，并生成所述授权结果信息。

[0023] 作为一个优选实施例，还可以预先保存 ACL(访问控制列表 (Access Control List，ACL)，作为一个实施例，该 ACL 表中可以预先存储请求方、接收方、服务名以及访问权限的相关数据，步骤 S102 中可以根据 ACL 表进行授权处理，生成授权结果信息，例如，如果 ACL 表中存储以下信息：请求方为 A、接收方为 B、服务名为打印、访问权限为允许，则当 A 请求 B 的打印服务时，即可生成允许授权信息。通过 ACL 表的引入，带来了以下好处：(1) 减少访问频率，提高访问效率。现有的不同应用间的每次通信，都需要进行授权访问，即使对于同一个服务的调用，不管通信多少次，就需要进行多少次授权。通过 ACL 表，因已存在授权信息，不需要进行每次的授权访问，减少访问频率，对于同一个服务的调用，只需进行一次授权，保存在 ACL 中，以后都不需要进行授权，可直接调用，提高访问效率。(2) 同时访问多服务时避免多次提示。目前，一个应用需要访问多个服务时，就需要对每个服务进行授权提示，进行多次操作，通过 ACL 表，不需要进行任何提示，同时可以一次性对多个服务请求访问进行授权操作，避免多次提示和多次授权操作。(3) 可以嵌套访问。目前，多个应用进行嵌套访问，当超过两次调用访问时，需要进行两次以上的访问跳转，进行授权操作，因此，无法重现第一次调用访问时的上下文环境，即无法实现超过两层调用访问的嵌套访问。通过 ACL 表，在进行嵌套访问时，由于每层访问，可以直接进行授权操作，不需要进行访问跳转，

即保留了每次调用访问时的上下文环境，从而实现嵌套访问。

[0024] 由于本发明预先保存了是否可以对某个应用授权或不授权的列表，通过区分受限资源和非受限资源，以及 ACL，引入黑白名单，因此本发明每个应用仅需一次授权判断，减少了访问控制干预频度，增强了用户体验。

[0025] 申请人在申请号为 201210094195.1，发明名称为《在线应用平台的进程通信方法、客户端、应用进程管理器》的专利申请中提供了在线应用平台上应用间通信的实现方案，作为一个优选实施例，本发明可以通过这种应用间通信的方式实现对应用的访问控制，过程如下：

[0026] 当在线应用平台上启动某个应用时，在线应用平台的客户端按照预定的通信协议创建应用进程；并记录该应用可处理的消息类型；应用进程是指该应用在客户端运行时的存在形态，包括应用进程 ID、应用名称、上下文空间、消息队列、可执行程序路径；消息队列为在线应用平台与该应用进程进行通信的载体。

[0027] 在线应用平台的客户端的授权结果信息可以通过发送方应用所对应的消息队列发送至发送方应用；发送方应用监控消息队列中的消息，如果授权结果信息为允许访问信息，则开始与接收方应用进行通信：

[0028] 首先构造消息并发送至在线应用平台的客户端，消息包括根据预定通信协议定义的应用名称、消息类型、消息体；客户端将收到的消息投递至接收方应用所对应的应用进程的消息队列中，接收方应用的应用进程监控消息队列中的消息，并进行处理；当发送方应用或接收方应用退出时，在线平台的客户端销毁所述应用进程。

[0029] 为了能够更加清晰的理解本发明，以下列举一个本发明的应用实例：

[0030] 应用 A 作为请求方需要与应用 B 进行访问，此时应用 B 为接收方。首先，在线应用平台的客户端创建应用 A 的进程 a，应用 B 的进程 b，应用 A 请求调用应用 B 的服务 C，此时应用 A 构造请求消息，包括根据预定通信协议定义的应用名称 B、消息类型 C、消息体，并发送至在线应用平台的客户端，客户端先检查应用 B 的黑白名单中是否有应用 A，如果在白名单中，即授权结果为允许，则进行通信，如果在黑名单中，即授权结果为拒绝访问，则发送拒绝访问消息给 A。如果应用 B 的黑白名单中均不存在应用 A，则在 ACL 表中，进行搜索，是否存在应用 B 将服务 C 授权给应用 A 的记录，如果存在，且授权记录为允许，则进行通信，如果不存在，则进行授权提示，用户授权为允许，则进行此应用间通信，用户授权为拒绝，则禁止此应用间通信。此时，若应用 A 需要同时访问应用 D、应用 E 等多个应用的服务时，将会统一在一个提示中，进行授权操作，避免多次提示授权。在进行提示授权操作后，将此次授权的结果记录在 ACL 表中，以便于下次的直接授权判断。达到每个应用仅需一次授权判断，减少了访问控制干预频度，增强了用户体验。

[0031] 与上述在线应用平台上应用间通信的访问控制方法相对应，本发明还提供了一种在线应用平台的应用进程管理器，用于实现在线应用平台内应用间的通信，所述应用进程管理器位于在线应用平台的客户端，应用进程管理器包括发送进程消息接口和访问控制装置。

[0032] 发送进程消息接口是与发送方应用或发送方应用通信的接口，发送方应用将访问请求发送至发送进程消息接口，访问控制装置对访问请求进行是否授权的处理，生成授权结果信息，并通过发送进程消息接口发送给发送方应用。

[0033] 作为一个实施例，应用进程管理器还包括第一存储装置，预先存储可授权应用列表；访问控制装置在可授权应用列表中查找发送方应用，如果找到，则生成允许访问信息。

[0034] 另外，作为一个实施例，应用进程管理器还可以包括第二存储装置，预先存储不可授权应用列表；访问控制装置如果在第二存储装置中找到发送方应用，则生成拒绝访问信息。

[0035] 作为一个优选实施例，所述应用进程管理器还包括第三存储装置，用于存储 ACL 表，所述 ACL 表为访问控制列表，用于存储请求方应用标识、接收方应用标识、服务名、访问权限；所述访问控制装置在预先存储的 ACL 表中查找所述发送方应用的服务，如果找到，则生成所述允许访问信息。

[0036] 图 2 为包含三种存储装置的原理框图。

[0037] 用户可以根据需求决定在实现应用进程管理器时保存哪种列表。作为一个优选实施例，访问控制装置如果在所保存的列表里未找到发送方应用，则提示用户是否对发送方应用授权，并根据用户的返回结果生成授权结果信息以及将发送方应用加入第一存储装置或第二存储装置。同样，应用进程管理器还包括实现申请号为 201210094195.1 的相应模块：

[0038] 当启动应用时，进程创建接口按照预定的通信协议创建应用进程；并记录应用可处理的消息类型；发送方应用经过授权后，将消息通过发送进程消息接口发送至接收方应用的消息队列中，接收方应用监控消息队列中的消息，并进行处理，进程销毁接口当所述发送方或接收方应用退出时销毁所述发送方或接收方应用的应用进程。

[0039] 上述实施例为本发明较佳的实施方式，但本发明的实施方式并不受上述实施例的限制，其他任何未背离本发明的精神实质和原理下所作的修改、修饰、替代、组合、简化，均应为等效的置换方式，都应包含在本发明的保护范围之内。

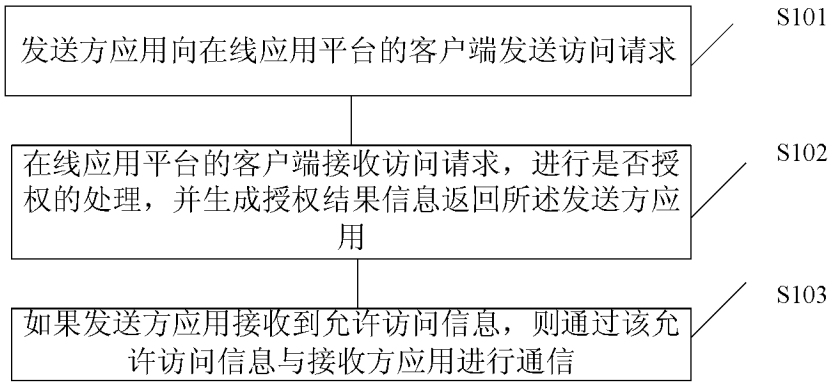

发送方应用向在线应用平台的客户端发送访问请求
S101
在线应用平台的客户端接收访问请求，进行是否授权的处理，并生成授权结果信息返回所述发送方应用
S102
如果发送方应用接收到允许访问信息，则通过该允许访问信息与接收方应用进行通信
S103

图 1

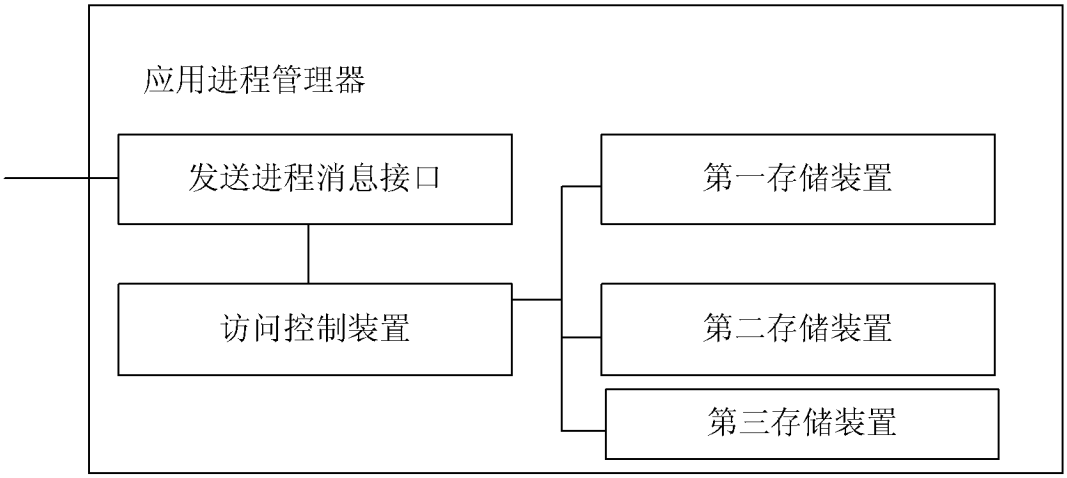

应用进程管理器
发送进程消息接口
访问控制装置
第一存储装置
第二存储装置
第三存储装置

图 2