[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
*G06F 21/22 (2006.01)*

[12] 发明专利说明书

专利号 ZL 200710032109.3

[45] 授权公告日 2009 年 7 月 29 日

[11] 授权公告号 CN 100520797C

[22] 申请日 2007.12.5
[21] 申请号 200710032109.3
[73] 专利权人 珠海金山软件股份有限公司
地址 519015 广东省珠海市珠海吉大景山路莲山巷 8 号金山电脑大厦
[72] 发明人 黄声声 邓 鹏
[56] 参考文献
US5835090A 1998.11.10
US2006/0041940A1 2006.2.23
CN1561037A 2005.1.5
CN1516016A 2004.7.28
审查员 曹姝妹

[74] 专利代理机构 广州新诺专利商标事务所有限公司
代理人 杨焕军

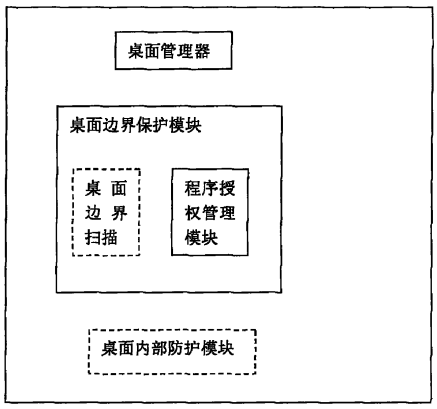
权利要求书 3 页 说明书 8 页 附图 2 页

[54] 发明名称

# 一种防止病毒动态攻击程序的装置和方法

[57] 摘要

本发明涉及计算机病毒防御技术，特别涉及一种防止病毒动态攻击程序的装置和方法。 一种防止病毒动态攻击程序的装置，其特征在于，所述装置包括：桌面管理器和桌面边界保护模块，所述桌面管理器为一受到所述桌面边界保护模块保护的桌面的列表；所述桌面边界保护模块用于监控与被保护桌面相关的操作。 通过上述技术方案本发明可以阻止病毒跨桌面进行攻击操作，如向其他桌面上的程序进行 Hooks、消息、伪造窗口的钓鱼攻击等，以确保此其他桌面中运行的程序难以被盗号木马等病毒动态攻击。



1、一种防止病毒动态攻击程序的装置，其特征在于，所述装置：

包括桌面管理器和桌面边界保护模块，所述桌面管理器为一受到所述桌面边界保护模块保护的桌面的列表；

创建一桌面，并将所述桌面加入到所述桌面管理器；

所述桌面边界保护模块用于监控与被保护桌面相关的操作；所述桌面边界保护模块包括一程序授权管理模块，所述程序授权管理模块根据其包含的已授权程序列表监控和/或拦截系统中线程或进程对被保护桌面相关操作的执行行为。

2、根据权利要求 1 所述的一种防止病毒动态攻击程序的装置，其特征在于，所述程序授权管理模块监控和/或拦截系统中线程或进程对被保护桌面相关操作的执行的行为包括以下三类行为中的一种或几种：打开被保护桌面；将线程或者进程设置到被保护桌面上运行；将进程创建到被保护桌面上。

3、根据权利要求 2 所述的一种防止病毒动态攻击程序的装置，其特征在于，所述程序授权管理模块具体通过监控和/或拦截如下 API 函数实现：

监控和/或拦截线程或进程打开被保护桌面，需要拦截 CreateDesktop、OpenDesktop 、OpenInputDesktop 中的一种或几种；监控和/或拦截线程或进程被指定到被保护桌面上运行，需要拦截 SetThreadDesktop；监控和/或拦截线程或进程被创建到被保护桌面上，需要拦截 CreateProcess、NTCreateProcess 、zwCreateProcess 中的一种或几种。

4、根据权利要求 1 所述的一种防止病毒动态攻击程序的装置，其特征在于，所述桌面边界保护模块还包括，对需要进入所述被保护桌面的程序进行安全检测的桌面边界扫描模块。

5、根据权利要求 1 所述的一种防止病毒动态攻击程序的装置，其特征

在于，所述装置还包括，对运行在所述被保护桌面上的程序进行行为隔离的桌面内部防护模块。

6、一种防止病毒动态攻击程序的方法，其特征在于，其包括如下过程：

创建一桌面管理器；所述桌面管理器为一受到桌面边界保护模块保护的桌面的列表；

创建一桌面；

将所述桌面加入到所述桌面管理器；

利用所述桌面边界保护模块对与所述桌面相关的操作进行监控，使所述桌面受到保护；

所述桌面边界保护模块包括一程序授权管理模块，所述程序授权管理模块根据其包含的已授权程序列表监控和/或拦截系统中线程或进程对与所述被保护桌面相关操作的执行行为。

7、根据权利要求 6 所述的一种防止病毒动态攻击程序的方法，其特征在于，所述程序授权管理模块监控和/或拦截系统中线程或进程对被保护桌面相关操作的执行的行为包括以下三类行为中的一种或几种：打开被保护桌面；将线程或者进程设置到被保护桌面上运行；将进程创建到被保护桌面上。

8、根据权利要求 7 所述的一种防止病毒动态攻击程序的方法，其特征在于，所述程序授权管理模块具体通过监控和/或拦截如下 API 函数实现：

监控和/或拦截线程或进程打开被保护桌面，需要拦截 CreateDesktop、OpenDesktop 、OpenInputDesktop 中的一种或几种；监控和/或拦截线程或进程被指定到被保护桌面上运行，需要拦截 SetThreadDesktop；监控和/或拦截线程或进程被创建到被保护桌面上，需要拦截 CreateProcess、NTCreateProcess 、zwCreateProcess 中的一种或几种。

9、根据权利要求 6 所述的一种防止病毒动态攻击程序的方法，其特征在于，所述桌面边界保护模块还包括，对需要进入所述被保护桌面的程序

进行安全检测的桌面边界扫描模块。

10、根据权利要求 6 所述的一种防止病毒动态攻击程序的方法，其特征在于，所述方法还包括，通过桌面内部防护模块对运行在所述被保护桌面上的程序进行行为隔离。

# 一种防止病毒动态攻击程序的装置和方法

## 技术领域

本发明涉及计算机病毒防御技术，特别涉及一种防止病毒动态攻击程序的装置和方法。

## 背景技术

随着病毒、蠕虫、木马、后门和混合威胁的泛滥，当前针对新漏洞的攻击产生速度比以前要快得多；而且由于黑客已经不再满足于从病毒爆发引起的网络瘫痪中获得成就感，而是希望从中获取经济利益，因此现在的病毒更为趋向于恶意代码攻击，包括间谍软件、网络欺诈、基于邮件的攻击和恶意 Web 站点等。例如在以前，病毒的类型中少数是具有控制和窃取功能的木马程序，因此多具有明显的破坏行为；而现在最活跃的病毒大部分是潜伏的恶意代码，在攻击行为上力求不被注意，目的是希望通过信息窃取和远程控制获得经济利益；身份信息窃取类代码则开始借助于网络钓鱼技术，通过窃取网上信用卡、银行帐号密码，以及用户的网游帐号等虚拟资产等信息对用户现实世界的经济利益造成损失。这些攻击往往伪装为合法应用程序和邮件信息，设计为欺骗用户暴露敏感信息、下载和安装恶意程序，传统的安全软件很难加以阻挡，往往需要先进的检测和安全技术。

## 发明内容

本发明的一个目的在于，提供一种防止病毒动态攻击程序的装置。

本发明该目的是通过如下技术方案实现的：

一种防止病毒动态攻击程序的装置，其特征在于，所述装置包括：

桌面管理器和桌面边界保护模块，所述桌面管理器为一受到所述桌面边界保护模块保护的桌面的列表；

所述桌面边界保护模块用于监控与被保护桌面相关的操作。

所述桌面边界保护模块包括，监控和/或拦截系统中线程或进程对被保护桌面相关操作的执行的程序授权管理模块。

所述程序授权管理模块监控和/或拦截系统中线程或进程对被保护桌面相关操作的执行的行为包括以下三类行为中的一种或几种：打开被保护桌面；将线程或者进程设置到在被保护桌面上运行；将进程创建到在被保护桌面上。

特别地，所述桌面边界保护模块还包括，对需要进入所述被保护桌面的程序进行安全检测的桌面边界扫描模块。

所述装置还包括，对运行在所述被保护桌面上的程序进行行为隔离的桌面内部防护模块。

本发明的另外一个目的在于，提供一种防止病毒动态攻击程序的方法。

本发明该目的是通过如下技术方案实现的：

一种防止病毒动态攻击程序的方法，其特征在于，其包括如下过程：

创建一桌面管理器；所述桌面管理器为一受到桌面边界保护模块保护的桌面的列表；

创建一桌面；

将所述桌面加入到所述桌面管理器；

利用所述桌面边界保护模块对与所述桌面相关的操作进行监控，使所

述桌面受到保护。

所述桌面边界保护模块包括，监控和/或拦截系统中线程或进程对被保护桌面相关操作的执行的程序授权管理模块。

所述程序授权管理模块监控和/或拦截系统中线程或进程对被保护桌面相关操作的执行的行为包括以下三类行为中的一种或几种：打开被保护桌面；将线程或者进程设置到在被保护桌面上运行；将进程创建到在被保护桌面上。

特别地，所述桌面边界保护模块还包括，对需要进入所述被保护桌面的程序进行安全检测的桌面边界扫描模块。

所述方法还包括，通过桌面内部防护模块对运行在所述被保护桌面上的程序进行行为隔离。

本发明通过在计算机操作系统中建立一桌面管理器，以及一个监控与桌面管理器中被保护桌面相关的操作的桌面边界防护模块，来监视或拦截系统中线程或进程对被保护桌面执行不当的操作。如在未授权的情况下修改系统中与被保护桌面相关的底层数据结构以及将线程或者进程设置到在被保护桌面上运行；将进程创建到在被保护桌面上等；通过上述技术方案本发明可以阻止病毒跨桌面进行攻击操作，如向其他桌面上的程序进行Hooks、消息、伪造窗口的钓鱼攻击等，以确保此其他桌面中运行的程序难以被盗号木马等病毒动态攻击。

附图说明

图 1 为本发明所述装置的原理示意图；

图 2 为本发明所述方法的流程图；

图 3 为本发明中所述桌面边界扫描流程图。

具体实施方式

**实施例一**

下面结合附图 1、2 具体的 Windows 操作系统，进一步阐述本发明的技术方案。

如图 1，一种防止病毒动态攻击程序的装置，所述装置包括： 桌面管理器和桌面边界保护模块，所述桌面管理器为一受到所述桌面边界保护模块保护的桌面的列表；所述桌面边界保护模块用于监控与被保护桌面相关的操作。所述桌面边界保护模块至少包括一用于监控和/或拦截系统中线程或进程对被保护桌面相关操作的执行的程序授权管理模块。

众所周知，利用 Windows 操作系统的计算机，在正常启动运行的条件下，会显示出一个可视的界面，本发明中将该界面定义为“主桌面”；所述“主桌面”除了包括显示在该界面上的各种快捷图标、文件或文件夹等外，还包括有支撑上述可视信息的底层数据信息，如程序列表、注册表信息、操作系统底层数据结构等。

如图 2，本发明用于防止病毒动态攻击程序的方案的过程如下：

在 Windows 操作系统中建立一桌面管理器，所述所述桌面管理器为一受到所述桌面边界保护模块保护的桌面的列表；

建立一有别于上述“主桌面”的受特殊保护的安全桌面；

将所述安全桌面加入到所述桌面管理器；

利用桌面边界保护模块对与所述桌面相关的操作进行监控，使所述安全桌面受到保护。

本实施例中，所述桌面边界保护模块的功能是通过其内部的用于监控和/或拦截系统中线程或进程对被保护桌面相关操作的执行的程序授权管理模块实现的。利用所述程序授权管理模块对系统中线程或进程访问安全桌面相关的操作进行监控或/和拦截，隔绝来自其他桌面的所有未经授权程序对所述安全桌面的常见攻击手段，如 Hooks、消息、伪造窗口的钓鱼攻击等，以确保此安全桌面中运行的程序难以受到上述病毒的动态攻击。在所述安全桌面中维护有一个被保护的程序列表，当一个程序被加入安全桌面，即此程序被加入了安全桌面的被保护程序列表，此列表明确了哪些程序需要保护。当在此列表中的程序，被采用保护模式运行的时候，所启动的进程就会被设为从属于安全桌面；在这种情况下，来自所述主桌面的 Hook 等攻击操作将不会影响这个进程。

具体说，为了隔绝病毒程序对所述安全桌面的攻击，所述程序授权管理模块拦截了所有未经过安全检测（通过杀毒或者在线文件校验等方法进行检测）的程序在运行时切换到所述安全桌面运行的行为。即通过桌面边界防护模块防止没有经过安全检测的程序在运行时切换到所述安全桌面，避免其他程序通过在运行时切换到所述安全桌面，获得在所述安全桌面上执行代码的权限。

所述程序授权管理模块监控和/或拦截系统中线程或进程对被保护桌面相关操作的执行的行为包括以下三类行为中的一种或几种：1）、试图打开安全桌面（例如，使用 OpenDesktop 打开安全桌面的句柄）；2）试图指定一个程序在安全桌面上运行（例如，通过 API SetThreadDesktop 将线程设置到安全桌面上运行）；以及，3）、将一个进程或者线程设置到安全桌面去运行（例如，在 CreateProcess 中将进程的启动桌面设置为安全桌面）。在所述程序授权管理模块中也包含一已授权程序列表，该列表的内容与所述

安全桌面中维护的被保护的程序列表相对应，用于判断哪些程序可以访问所述安全桌面。即所述程序授权管理模块隔绝了非可信任程序对安全桌面的访问，这使得未经认证或者杀毒的程序无法进入安全桌面，避免了木马通过潜入安全桌面进行攻击的可能。目前本发明的产品实现中，具体包括两种做法，可以是其中任何一种，或者是两种方法的结合：

做法 1 是拦截几个相关的系统 API 函数：

| 目的 | 拦截函数 |
|---|---|
| 监控和/或拦截线程或进程打开安全桌面 | CreateDesktop |
| | OpenDesktop |
| | OpenInputDesktop |
| 监控和/或拦截线程或进程被指定到安全桌面上运行 | SetThreadDesktop |
| 监控和/或拦截线程或进程被设置到安全桌面上 | CreateProcess |
| | NTCreateProcess |
| | zwCreateProcess |

做法 2 是采用拦截系统中用于枚举系统中的桌面 API 的函数并且对安全桌面采用随机桌面名称的方法实现。

**实施例二**

本实施例与实施例一的区别在于，所述桌面边界保护模块中还包括一桌面边界扫描模块。如实施例一所述，由于所述安全桌面设计的基本原则是从操作系统当中隔离出一个可信安全区域，因此对于进入安全区域的程序必须经过安全检测方能放行。该检验过程基于杀毒或者在线文件校验等方法进行；无论是杀毒或者在线文件校验，都是为了查询被检测程序是否为已知的安全程序。作为进一步方案，本发明是在通过隶属于所述桌面边界保护模块的桌面边界扫描模块实现，所述采用桌面边界扫描模块对需要进

入所述安全桌面的程序进行安全检测；辅助所述程序授权管理模块在所述安全桌面中维护有一可信的程序列表。如图 3 所示，对被需要加入所述安全桌面的程序进行判断，假如是安全程序，则将其加入安全桌面之中；假如返回为非安全程序，则拒绝将此文件加入安全桌面列表。假如此程序未知，则在征得用户同意的情况下通过相关手段传送给杀毒或者在线文件校验软件的提供商。

**实施例三**

本实施例与实施例一的区别在于，所述防止病毒动态攻击程序的装置还包括一桌面边界扫描模块。

为了处理所述安全桌面中运行的经过安全检测的程序由于漏洞或者用户的不当操作等原因将引入木马等动态攻击性病毒的可能性，在所述装置中还包括一桌面内部防护模块，所述桌面内部防护模块对所述安全桌面中各个进程的危险操作行为进行行为隔离，防止由于漏洞感染木马等动态攻击性病毒的程序借机攻击其他受保护的程序进程，即防止各个程序对其他程序进行高危险性操作的可能。

由于所述桌面内部防护模块的存在，当一个进程在所述安全桌面中执行一个可能影响其他进程的操作时，所述桌面内部防护模块将根据其权限大小加以阻止或者放行。高权限的进程可以执行影响低权限进程或者与自身同级别进程的操作，低权限进程则不能影响高权限进程，这就是上文所说的行为隔离。举例说明：当低权限的 IE 浏览器进程试图使用 API OpenProcess()访问高权限的安全桌面进程时，由于其权限不足，则内部防护

模块将阻止这一操作；反过来，当安全桌面的内部模块试图使用 API OpenProcess()访问低权限的 IE 浏览器进程时，内部防护模块将对此操作加以放行。具体哪些模块拥有哪个等级的权限，由具体产品采用的策略决定。一般而言，遵循的原则是：访问的内容比较繁杂，容易由于漏洞而被攻破的程序，如浏览器等，授予较低的权限；而行为较为单纯一致，变化较少，功能比较重要的程序，如进程管理器等，授予较高的权限。

**实施例四**

在利用 WindowsNT 系列的操作系统的计算机中，在正常启动完成后，默认会创建一个登录桌面 Winlogon，尽管一般而言，由于操作此桌面所需的权限较高，病毒难以攻击此桌面，但是当病毒使用各种漏洞将自身的权限提高后，就可以自由的在 Winlogon 桌面上使用 Hooks、消息、伪造窗口的钓鱼攻击等手段进行攻击了；如果通过将该桌面加入到所述桌面管理器，所述桌面边界边界保护模块就可以保证即使病毒将自身权限提高的情况下也无法使用 Hooks、消息、伪造窗口的钓鱼攻击等手段进行攻击。

本发明还有一些其他的变形，如果本领域的技术人员受到本发明的启发，不脱离本发明精神和范围的任何修改或局部替换，均应涵盖在本发明的保护范围当中。

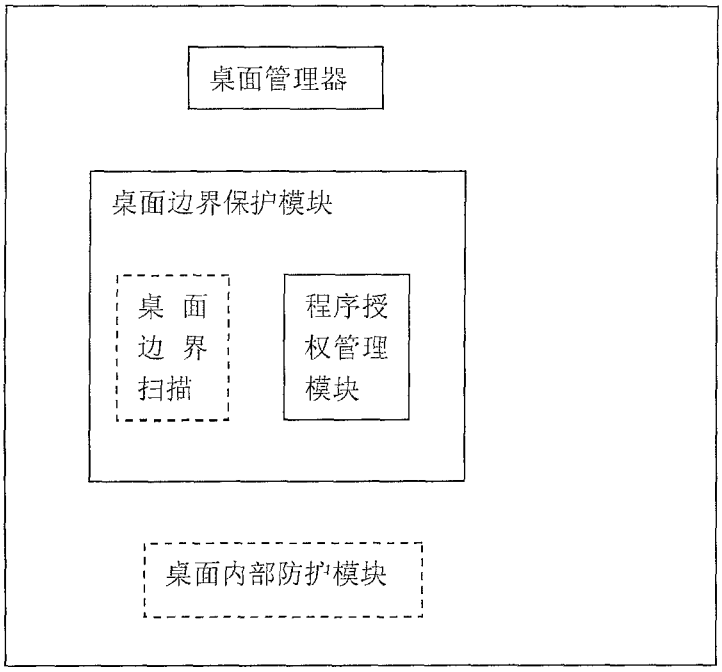

桌面管理器
桌面边界保护模块
桌面边界扫描
程序授权管理模块
桌面内部防护模块

图 1

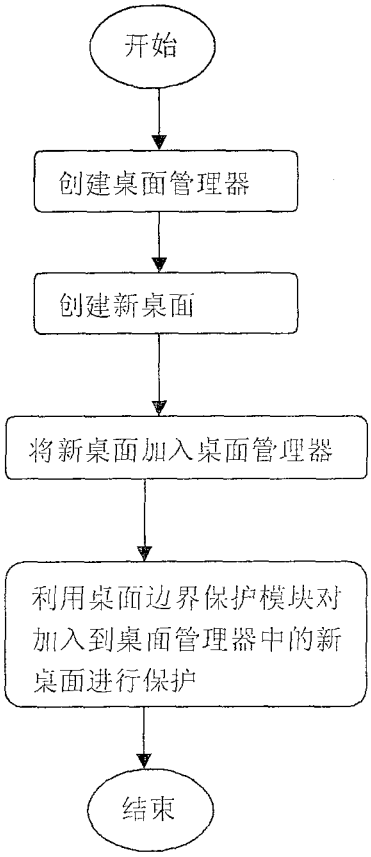

开始
创建桌面管理器
创建新桌面
将新桌面加入桌面管理器
利用桌面边界保护模块对加入到桌面管理器中的新桌面进行保护
结束

图 2

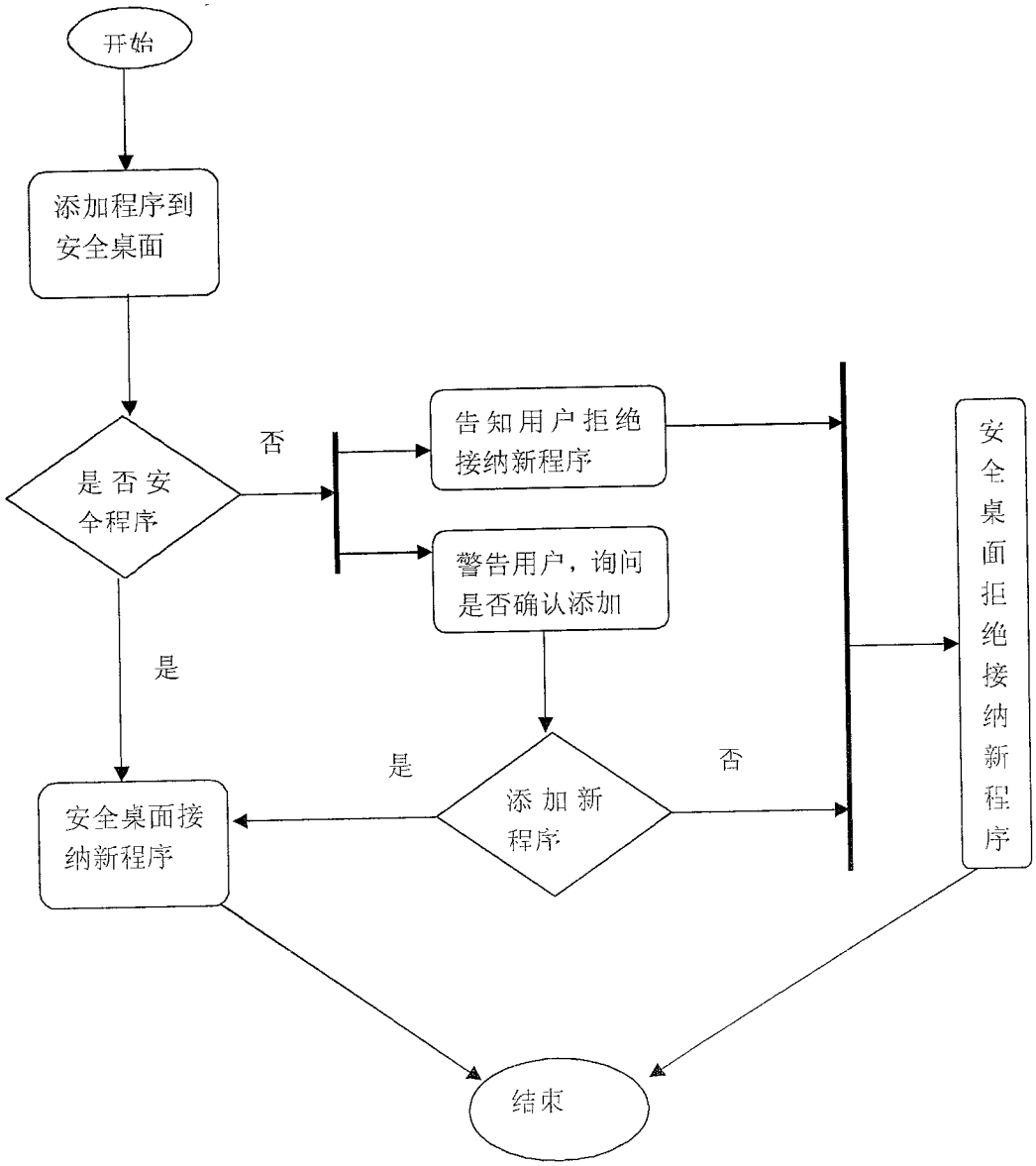

开始
添加程序到安全桌面
是否安全程序
否
告知用户拒绝接纳新程序
警告用户，询问是否确认添加
是
是
添加新程序
否
安全桌面接纳新程序
安全桌面拒绝接纳新程序
结束

图 3