(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 101753545 A
(43)申请公布日 2010.06.23

(21)申请号 200810239181.8

(22)申请日 2008.12.11

(71)申请人 北京奇虎科技有限公司
地址 100025 北京市朝阳区建国路71号惠通时代广场D1

(72)发明人 潘剑锋 邹贵强 刘颖 张森 陆剑锋

(74)专利代理机构 北京海虹嘉诚知识产权代理有限公司 11129
代理人 张涛

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/26(2006.01)
G06Q 30/00(2006.01)

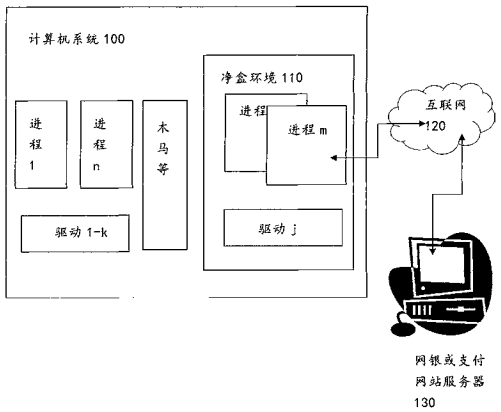
权利要求书 1 页 说明书 7 页 附图 4 页

(54)发明名称

净盒技术

(57)摘要

本发明涉及一种信息安全技术，尤其是一种净盒技术，其通过为用户的待执行对象开辟出一安全执行环境，并于安全执行环境中实行准入和禁入策略的方式，彻底地杜绝了任何病毒、恶意软件、木马或盗号程序等获取用户任何信息的可能性，并不需硬件成本的额外支出。就像是建立一个无尘的实验室进行实验一样，净盒为用户提供了一个可以放心进行信息交互或金融支付等的安全环境。



CN 101753545 A

1. 一种提供信息安全的方法，其特征在于包括：

启动待执行对象；

相应于待执行对象的启动，开启净盒，所述净盒是为待执行对象的执行所提供的安全环境；

将所述待执行对象调入所述安全环境，并执行待执行对象。

2. 根据权利要求 1 的方法，其特征在于：

所述安全环境的提供是通过新建进程或基于虚拟或复制技术实现的。

3. 根据权利要求 1 的方法，其特征在于：

还包括：放行与待执行对象相关的必要模块或行为，此外所有的模块或行为一律予以屏蔽或禁止的步骤。

4. 根据权利要求 3 的方法，其特征在于：

所述与待执行对象相关的必要模块或行为的认定是基于白名单实现的。

5. 根据权利要求 4 的方法，其特征在于：

还包括跟踪更新所述白名单的步骤。

6. 根据权利要求 1-5 之一的方法，其特征在于：

还包括开启净盒前验证与待执行对象相关的必要模块或行为的相关验证步骤。

7. 根据权利要求 5 的方法，其特征在于：

所述相关验证的验证内容包括但不限于：相关应用程序的一致性、待执行对象的一致性与正确性、以及待执行对象服务商的正确性。

8. 一种根据权利要求 1-7 之一的方法提供信息安全的系统。

9. 一种净盒装置，其特征在于包括：

为待执行对象提供安全环境的模块；

将所述待执行对象调入所述安全环境，并执行所述待执行对象的模块；以及，

在所述待执行对象调入所述安全环境之前以及执行所述待执行对象的过程中，放行与待执行对象相关的必要模块或行为，此外所有的模块或行为一律予以屏蔽或禁止的模块。

10. 根据权利要求 9 的净盒装置，其特征在于：

所述安全环境是通过新建进程或基于虚拟或复制技术提供的。

11. 根据权利要求 9 的净盒装置，其特征在于：

所述与待执行对象相关的必要模块或行为的认定是基于白名单实现的。

12. 根据权利要求 11 的净盒装置，其特征在于：

还包括跟踪更新所述白名单的模块。

13. 根据权利要求 9-12 之一的净盒装置，其特征在于：

还包括开启净盒前验证与待执行对象相关的必要模块或行为的相关验证模块。

14. 一种基于权利要求 9-13 之一的净盒装置提供信息安全的方法，其特征在于包括：

为待执行对象提供安全环境的步骤；

将所述待执行对象调入所述安全环境，并执行所述待执行对象的步骤；以及，

在所述待执行对象调入所述安全环境之前以及执行所述待执行对象的过程中，放行与待执行对象相关的必要模块或行为，此外所有的模块或行为一律予以屏蔽或禁止的步骤。

净盒技术

技术领域

[0001] 本发明涉及信息安全领域。

背景技术

[0002] 随着互联网技术的广泛应用，电子商务 (B2B，B2C，C2C)、电子支付、网上银行等日益成为互联网的重要应用模式之一。这使得客户与商家、客户与客户、商家与商家之间的信息交互，例如金融支付等的安全问题成为一个重大的问题。

[0003] 目前针对涉及电子商务操作的主要攻击手段包括：

[0004] 1、钓鱼，是指攻击者通过伪造或模拟一个界面与被攻击网站类似的网站，诱骗用户输入帐号密码等关键信息，从而达到窃取信息的目的。

[0005] 2、浏览器插件 / 注入攻击，攻击者通过向浏览器插入浏览器插件或注入浏览器进程，从而截获浏览器向服务器发送的帐号，密码等信息。

[0006] 3、键盘记录器，可以截获用户用键盘输入的敏感信息，密码安全控件由于技术上的局限性，仅能提供较简单防护，恶意程序通过钩子程序或驱动程序可以轻易绕过安全控件的保护。

[0007] 相应的，现有技术中所提供的安全支付的解决方案主要存在如下的一些做法：

[0008] 1、用防病毒软件来检测盗号和键盘记录 (keylogger) 等木马和间谍软件；

[0009] 2、在防病毒技术上衍生出来的密码安全控件；

[0010] 3、第三方验证，诸如短信验证码、一次一密等；

[0011] 4、数字证书验证或 USB 数字证书等。

[0012] 然而，这些解决方案均存在保护效果不佳或成本过高的问题。诸如在公开号为 CN101206779A 的中国申请中，采用了数字键盘模块，显示设备，USB 接口模块等安全支付技术。其虽然避开了使用网上银行时对计算机键盘的依赖，并与 USB_KEY 等工具兼容，提高了金融操作的安全性，但仍然存在三方面缺陷：

[0013] 其一，在用户登录时，恶意软件，如木马、远程监控、病毒等一系列非法手段仍然可以采用特定的手段，如监听内核驱动程序、截屏等，从计算机上获取用户密码等私人资料。这是由于数字键盘等尽管可以避免对计算机固有键盘的依赖，但其仍不可避免地需要使用诸如显示设备、内核驱动等计算机运行所必备的部件或程序，这就为恶意软件的入侵提供了可趁之机。

[0014] 其二，现有的各种安全支付的解决方案主要侧重于用户登录时的身份检验 / 验证，即入口验证。当用户利用数字键盘、USB_KEY、数字证书等进入交易系统后，现有技术无法确保用户在交易过程中的信息不被盗取或非法利用。诸如，在用户 A 利用某银行的转帐系统向用户 B 转帐的过程中，高超的恶意软件可以潜入支付进程并在用户 A 点击确定发送之前，将用户 B 的帐号更改。

[0015] 其三，由于 USB_KEY 等手段均需额外的硬件支持，因而其不可避免地会导致使用成本的增加。

[0016] 此外，对于第三方验证的方式而言，其除了保护效果不佳之外，仍然会存在第三方是否可确信的风险，而且由于需要与交易之外的第三方相互通信、验证等，其交易的手续及过程也过于繁琐，从而增加了风险成本与交易成本。

[0017] 经调查统计，现有人群中，仅有不到 10％的人经常采用网上银行等进行金融交易，与此相对的是，多达 90％的人出于对电子商务安全性或复杂性的担忧而不愿通过网络进行任何金融交易操作。

发明内容

[0018] 有鉴于此，亟需提供一种保护效果优越并不需额外成本支出的信息安全保护技术，以为用户提供全面、放心的信息交互或安全支付的保护，进而促进互联网应用，诸如信息交互、金融支付、电子商务、网上银行等的快速健康发展。

[0019] 为实现上述目的，本发明提出一种净盒 (Clean-Box) 技术，其通过为待执行对象开辟出一安全运行环境的发明构思，使用户的敏感信息免于恶意软件、木马、远程监控、病毒等的侵袭。其发明构思巧妙，简单易行，且其保护效果远优于现有的解决方案。

[0020] 本发明的第一方面在于提供一种提供信息安全的方法，其包括 ：

[0021] 启动待执行对象 ；

[0022] 相应于待执行对象的启动，开启净盒，所述净盒是为待执行对象的执行所提供的安全环境 ；

[0023] 将所述待执行对象调入所述安全环境，并执行待执行对象。

[0024] 本发明的第二方面在于提供一种基于第一方面方法提供信息安全的系统。

[0025] 本发明的第三方面在于提供一种净盒装置，其特征在于包括 ：

[0026] 为待执行对象提供安全环境的模块 ；将所述待执行对象调入所述安全环境，并执行所述待执行对象的模块 ；以及，在所述待执行对象调入所述安全环境之前以及执行所述待执行对象的过程中，放行与待执行对象相关的必要模块或行为，此外所有的模块或行为一律予以屏蔽或禁止的模块。

[0027] 本发明的第四方面在于提供一种提供信息安全的方法，其特征在于包括 ：为待执行对象提供安全环境的步骤 ；将所述待执行对象调入所述安全环境，并执行所述待执行对象的步骤 ；以及，在所述待执行对象调入所述安全环境之前以及执行所述待执行对象的过程中，放行与待执行对象相关的必要模块或行为，此外所有的模块或行为一律予以屏蔽或禁止的步骤。

[0028] 与现有技术相比，本发明通过净盒 (Clean-Box) 技术彻底地杜绝了任何病毒、恶意软件、木马或盗号程序等获取用户任何信息的可能性。就像是建立一个无菌的手术室来进行手术或无尘的实验室进行实验一样，净盒为用户提供了一个可以放心进行诸如电子商务、电子支付、网上银行等的安全环境。

附图说明

[0029] 下面将参照附图对本发明的具体实施方案进行更详细的说明，其中 ：

[0030] 图 1 为包含本发明净盒技术的计算机系统的结构示例图 ；

[0031] 图 2 为本发明净盒技术第一实施例的流程示意图 ；

[0032] 图 3 为本发明净盒技术第二实施例的流程示意图。

[0033] 图 4 为本发明净盒技术的模块架构示意图。

具体实施方式

[0034] 为了使本发明的目的、技术方案及优点更加清楚，以下结合附图以及实施例对本发明的净盒技术的优选方案进行详细说明。应当理解，此处所描述的具体实施方式仅仅是用来解释本发明的净盒技术的发明构思，并不用于限定本发明。

[0035] 图 1 为包含本发明净盒技术的计算机系统的结构示例图。如图 1 所示，计算机系统 100 通过互联网 120 与网上银行或支付网站服务器 130 相连，并运行有多个进程 1-n、驱动 1-k。作为示意，该计算机系统 100 中潜伏有一木马程序，该木马程序可能采取的攻击可以是钓鱼攻击、BHO 过滤攻击、键盘记录器以及其他任何可能的攻击手段。

[0036] 当用户通过金融支付软件或其他信息交互工具与外界（如，互联网 120、网上银行或支付网站服务器 130 等）进行信息交互时，计算机系统 100 创建一供金融支付软件或其他信息交互工具运行的净盒环境 110。在该净盒环境 110 中，与金融支付软件或其他信息交互工具相关的进程 m、驱动 j 等能够进入并运行，除此之外，木马等恶意软件以及其他的不相关进程 1-n、驱动 1-k 等模块或行为皆被屏蔽于净盒环境 110 之外，由此为用户提供了一个可以放心进行诸如电子商务、电子支付等的安全环境，并能确保用户私密信息的安全。

[0037] 图 2 为本发明净盒技术第一实施例的流程示意图。如图 2 所示，当用户想通过互联网 200 与网上银行 300 进行支付交付时，步骤 s200，用户于计算机系统 100 中启动交易程序。

[0038] 在步骤 s210 中，基于本发明的净盒 (Clean-Box) 理念，在计算机系统 100 中创建一净盒，即安全环境。

[0039] 步骤 s220 中，在上述创建的安全环境中执行准入和禁入策略。

[0040] 步骤 s230 中，于安全环境中调用交易相关工具并实施交易。

[0041] 步骤 s240 中，完成后退出净盒。

[0042] 由上述对本发明的阐述可知，与现有技术中所提供的安全支付的解决方案相比，本发明的净盒技术摒弃了传统的病毒防治理念，不再是被动应对层出不穷的各类恶意软件，进而不断耗费人力、物力一一研究恶意软件的攻击手段或病毒特性，并相应不断推出防治某病毒的软件或升级补丁。而是变被动为主动，于相应交易或软件执行之前创建一新的安全环境，并且在该安全环境中仅允许与执行对象，如交易或软件相关的必要的模块或行为发生，此外的所有模块或行为一律予以屏蔽或禁止。由于能进入到安全环境中的仅仅是与交易或软件相关的必要的模块或行为，这就杜绝了任何病毒、恶意软件、木马或盗号程序等获取用户任何信息的可能性，实现简单易行、不需额外成本即能充分保护用户信息安全的目的。

[0043] 本发明中，创建一个净盒 (Clean-Box)，即新的安全环境的手段或方案可以通过多种方式实现，例如针对特定一款应用软件（如某商业银行的网银支付软件）或交易，当交易或应用软件启动时，开启一个全新的进程作为安全环境。

[0044] 优选的，针对安全隐患尤为严重的计算机系统，本发明提出创建安全环境的方式为，在系统内复制或新建一个安全、干净的系统。例如 :利用虚拟技术如 VMWare 在 Windows、

Linux 等计算机系统 100 内再运行一个全新的 Windows 或 Linux 子系统，再把相应的交易置入该环境来运行。这样可以彻底隔绝母系统中的诸如木马、病毒或恶意软件攻击到子系统的交易操作。

[0045] 此外，本发明在创建出新的子系统后，也可进一步冻结外部母系统的任何运行。即，全新的子系统在执行交易操作期间，保持子系统外部环境的相对安静，使所有或潜伏或活跃于母系统的木马、病毒或恶意软件丧失激活并做出任何动作的可能性，由此为用户的金融操作提供更佳的安全保护。

[0046] 本发明所执行的准入和禁入策略为：仅允许与执行对象相关的必要的模块或行为发生，此外的所有模块或行为一律予以屏蔽或禁止。

[0047] 在通常情况下，大部分的金融交易操作是基于特定交易服务商所提供的交易软件进行的，如某银行的网银系统。因此，作为示例，对于必要的模块或行为的认定，可以基于白名单的方式进行。所述白名单是基于特定一款应用软件的交易服务商所提供的信息产生。这一信息中包含了运行该应用软件不可或缺的模块或行为。例如，某银行推出一款网银支付软件，并许可下列模块或行为支撑该网银支付软件的运行：

[0048] 交易相关的程序；

[0049] 与交易相应的特定网络数据流；

[0050] 完成交易所需的应用程序如浏览器等。

[0051] 由此，基于上述交易服务商所提供的许可信息产生用于本发明准入和禁入策略的白名单。在所创建的安全环境中执行交易期间，仅允许记载在白名单中的模块或行为进入安全环境或于安全环境中发生，而对未记载在白名单中的其他一切情形，则一律屏蔽或禁入。这里需要指出的是，交易服务商（如某银行）具有法定的权威性和可信性，而且其所提供的有关交易软件的许可执行的模块或行为的信息是所有恶意软件无法攻击或篡改的。本发明的准入和禁入策略巧妙利用这一情形，构建安全环境的完美屏障，在保障交易正常进行的同时，为用户提供最完善的信息保护。

[0052] 以基于浏览器的网上交易为例，本发明的准入和禁入策略可以是：

[0053] 仅允许：

[0054] a、交易相关的程序如支付程序或网银程序；

[0055] b、交易保护模块如密码保护控件；

[0056] c、其他必要的安全保护程序，诸如墨者免疫革离术等特定的安全软件，用于防止未被授权的程序调用，如防止 SetWindowsHookEx 被恶意调用；

[0057] d、与交易相应的合法的网络数据流；

[0058] e、为完成交易必须的系统程序如浏览器以确保交易程序能正常运行；

[0059] f、完成交易的程序与系统进程之间必要的通信。

[0060] 而以下模块或行为将被屏蔽和禁止：

[0061] a、应用层钩子程序；

[0062] b、不相干的系统驱动程序；

[0063] c、不必要的进程间通信；

[0064] d、不同于交易的网络数据流。

[0065] 可见，基于本发明的准入和禁入策略，由于净盒通过权限控制机制（准入和禁入

策略）防止消息钩子和恶意的驱动程序的装载，因此可有效免除诸如键盘记录器等的基于计算机硬件攻击用户敏感信息的可能。

[0066] 此外，对于其他的信息交互情形，如用户之间的文件传送、信息交互等，本发明的准入和禁入策略基于同样的原理构建，即，仅允许与执行对象相关的必要的模块或行为发生，此外的所有模块或行为一律予以屏蔽或禁止。所述必要的模块或行为可以基于信息交互双方或之一所信赖、并许可的内容来确定，也可以基于交互工具本身或交互工具发布商所特定的许可信息来确定。

[0067] 优选的，作为对本发明准入和禁入策略的辅助和补充，本发明在实行准入审核的同时利用黑名单实行禁入限制，该黑名单可以是累积的，针对某一款特定交互软件（包括交易软件）的常见的病毒攻击手段或其本身的特征信息，也可以是相应某一交互软件的特定防护需求（如安全等级的需求）而罗列的特定防范对象。由此可以在符合黑名单记载的情形发生时，优先将明确禁入的对象排除在安全环境之外。从而节约判定流程的时间，并进一步保障用户信息的安全。

[0068] 优选的，本发明还可提供针对特定对象或用户的跟踪更新手段，以此保持准入和禁入策略的及时性、准确性。对于特定交易服务商而言，当其进行系统升级或交易软件更新等情形时，本发明跟踪其许可信息的可能的变更，并在变更出现时同步更新准入和禁入策略，如白名单，以此防止某些高超的恶意软件利用交易服务商信息变更的机会非法获取用户信息。

[0069] 图 3 为本发明净盒技术第二实施例的流程示意图。与第一实施例不同的是，本发明的第二实施例中，在交易启动后、安全环境创建之前，验证与交易或软件相关的必要的模块或行为。即，在图 2 的步骤 200 与步骤 210 之间，对于那些准入净盒的，运行该交易软件不可或缺的模块或行为进行验证。这一验证的优点在于可以进一步确保创建的净盒未受感染或避免净盒受感染。

[0070] 如图 3 所示，用户在步骤 s300 中启动交易。

[0071] 在步骤 s310 中进行相关验证，具体的验证内容包括：

[0072] 1、验证相关应用程序的一致性，以确保如浏览器、交易程序等未被修改。

[0073] 验证的手段可以是数字签名验证或 MD5 验证等。

[0074] 以目前的 BHO 过滤攻击为例，由于 BHO 过滤攻击需要在浏览器中插入恶意模块，但本发明的净盒技术具有模块认证技术，其通过验证相关应用程序的一致性，仅允许与浏览器自身的模块和与交易相关的模块的加载，除此之外，任何恶意的模块都无法加载，由此可有效免除诸如 BHO 等恶意软件的攻击。

[0075] 2、验证交易提供商。

[0076] 验证的手段可以是数字证书验证等。

[0077] 众所周知，数字证书是交易提供商网络运营的特定属性之一，任何钓鱼网站均不可能获得被攻击站点的证书，本发明的净盒技术通过数字签名与证书验证机制可有效免除任何基于伪造手段的钓鱼攻击。

[0078] 3、验证交易程序的一致性和正确性。

[0079] 验证的手段可以是签名验证，也可以是其他的脚本验证方式。基于交易脚本的一致性和正确性的验证，可进一步防止交易脚本本身被恶意软件利用的可能。

[0080] 若上述步骤 s310 中的相关验证存在问题，如交易脚本不一致或交易提供商证书系伪造等，则停止交易程序，可选地向用户提供文字通知或语音提示验证失败的信息，并转入步骤 s350 结束流程。

[0081] 若上述步骤 s310 中的相关验证通过，则于步骤 s320 中开启新的进程作为安全环境。

[0082] 步骤 s330 中，执行准入和禁入策略，包括：加载交易程序及模块；屏蔽所有浏览器插件，应用层钩子；开启网络数据监控；开启进程间通信监控等。

[0083] 步骤 s340 中，加载交易脚本，并实施交易。

[0084] 步骤 s350 中，交易完成或相关验证失败，退出净盒。

[0085] 至此，本发明第二实施例通过相关验证进一步确保了用户信息安全。当计算机系统 100 出现较为严重的安全隐患，或用户进行较为重要的信息交互、金融支付时，包括相关验证手段的净盒技术可为用户提供最佳的信息安全保障。

[0086] 图 4 为本发明净盒技术的模块架构示意图。如图 4 所示，安全设置 / 策略库 400 中包含有涉及计算机信息安全的各种安全设置及安全策略等。准入和禁入控制模块 410 基于安全设置 / 策略库 400 获得与启动的交易程序相关的准入和禁入策略（未图示）。在净盒 / 安全环境 440 创建之前，相关验证模块 420 针对准入和禁入控制模块 410 所获得的准入和禁入策略中认可的与交易或软件相关的必要的模块或行为进行安全验证。作为示例，这一安全验证基于静态验证模块 421、及动态验证模块 422 实现。其中，静态验证模块 421 根据安全策略，通过静态技术验证执行对象及其相关资源，包括但不局限于模块验证；动态验证模块 422 根据安全策略，通过动态技术验证执行对象及其相关资源，包括但不局限于执行对象的一致性与正确性验证，执行对象服务商的正确性验证，执行对象行为的验证等。

[0087] 结合图 3、4，当相关验证未通过或存在问题时，停止交易的执行并向用户提示相关验证失败等信息。至此交易结束，由用户或交易服务商对验证未通过的模块或行为进行替换或修补，待替换或修补完善后，重新启动交易。

[0088] 此外，可选地，当相关验证未通过或存在问题时，暂停交易程序的继续执行，向用户提供风险提示信息并根据用户选择确定是否继续执行交易程序。所述风险提示信息可根据安全设置 / 策略库 400 中包含的安全设置 / 策略向用户提示当前系统的风险等级、以及可行性建议等。例如，由于 BHO 过滤攻击在浏览器中插入了恶意模块而造成相关应用程序的不一致，即，浏览器被修改，但净盒技术可以通过静态验证模块 421、动态验证模块 422 或其他的安全保护程序，如墨者免疫革离术等将该恶意模块屏蔽而不影响交易程序的安全执行，此时基于安全设置 / 策略库 400 可向用户提示风险等级为低，并建议用户继续执行交易程序。由此，用户可根据风险提示信息选择是否继续执行交易，从而避免了在信息安全允许的范围内，出现诸如用户急需金融转帐却无法启动执行交易程序的困境。

[0089] 当相关验证通过或用户选择继续交易时，由净盒创建模块（未图示）创建净盒，为待执行对象提供安全环境。访问隔离模块 430 作为净盒的安全屏障，基于准入和禁入控制模块 410 获取的与该交易或软件相关的准入和禁入策略，放行与交易或软件相关的必要的模块或行为，并屏蔽或禁止此外所有的模块或行为，以隔绝交易或软件及其相关资源与外界的不必要通信，如不必要的进程间通信、不同于交易的网络数据流等。此后，交易程序或软件在创建的净盒 / 安全环境 440 中运行并实现信息的安全交互。

[0090] 应理解的是，本发明的上述各具体实施例中所涉及的各处理流程可以构建为相应的装置或模块。而各模块之间的关联方式也可以是本发明具体实施例部分的任意一种方式。

[0091] 此外，在此描述的本发明可以有许多变化，这种变化不能认为偏离本发明的精神和范围。因此，所有对本领域技术人员显而易见的改变，都包括在本权利要求书的涵盖范围之内。

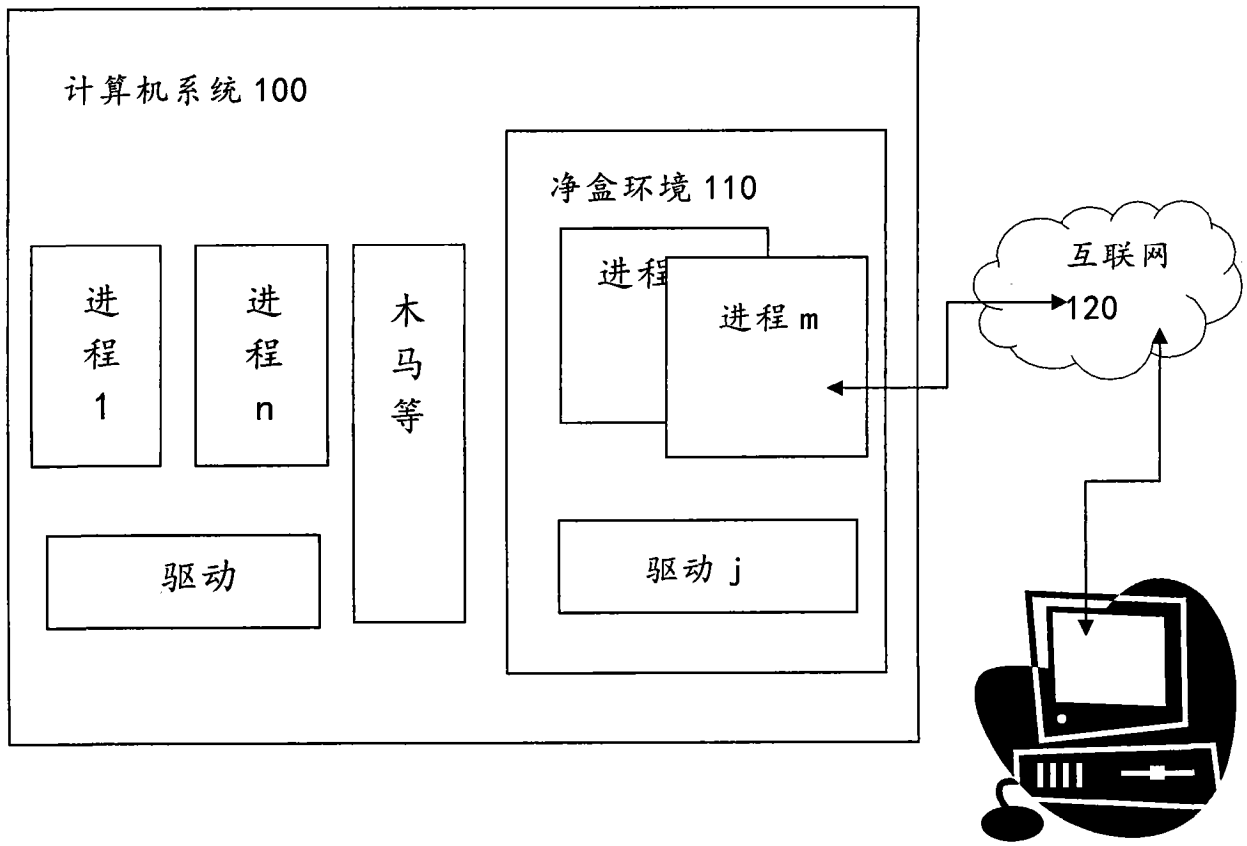

计算机系统 100
进程 1
进程 n
木马等
驱动
净盒环境 110
进程
进程 m
驱动 j
互联网
120
网银或支付网站服务器 130

图 1

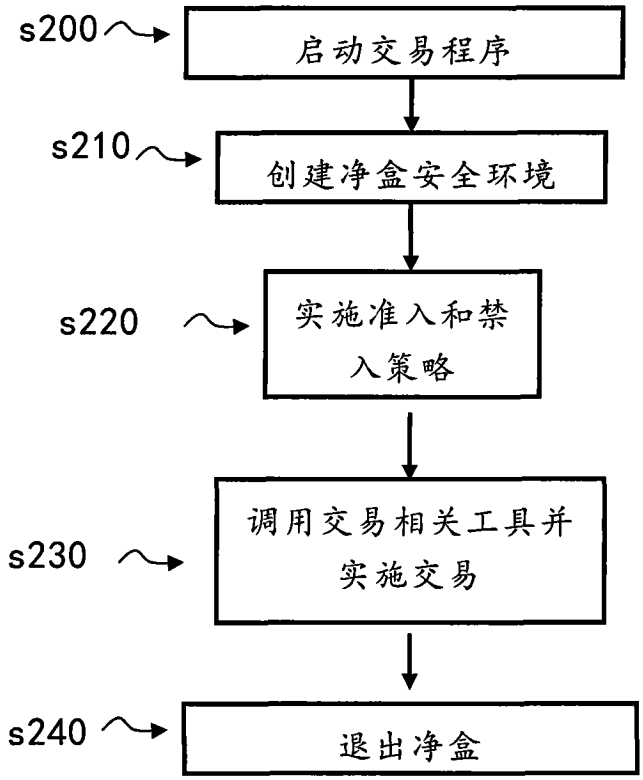

s200
启动交易程序
s210
创建净盒安全环境
s220
实施准入和禁入策略
s230
调用交易相关工具并实施交易
s240
退出净盒

图 2

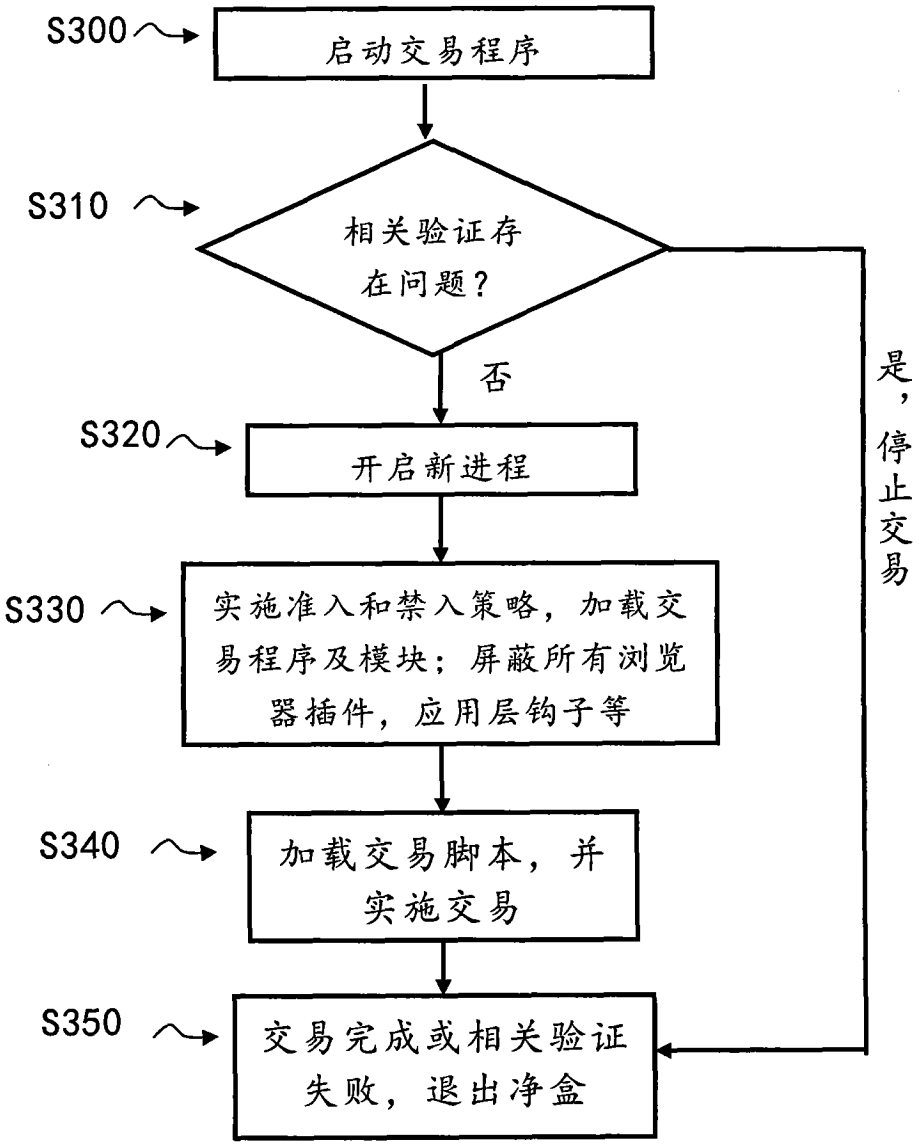

S300
启动交易程序
S310
相关验证存在问题？
否
是，停止交易
S320
开启新进程
S330
实施准入和禁入策略，加载交易程序及模块；屏蔽所有浏览器插件，应用层钩子等
S340
加载交易脚本，并实施交易
S350
交易完成或相关验证失败，退出净盒

图 3

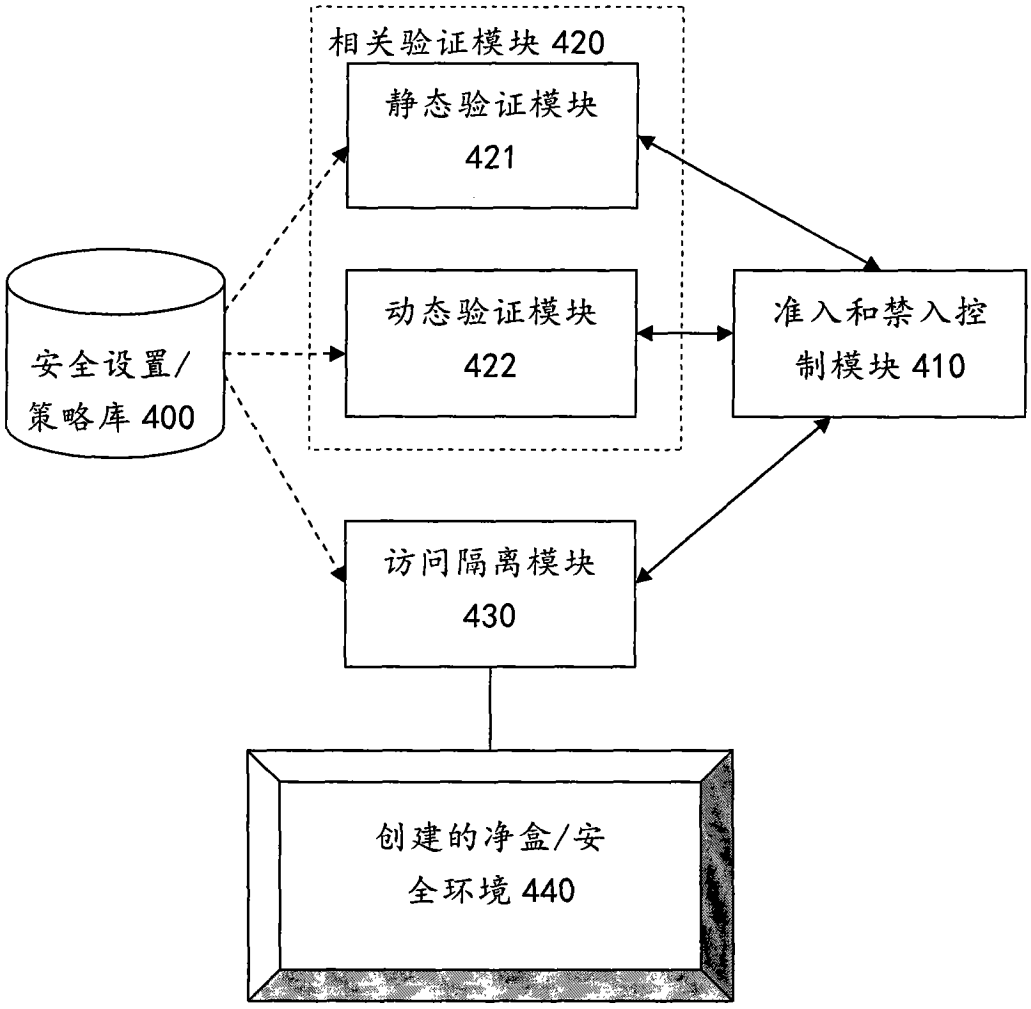

相关验证模块 420
静态验证模块 421
动态验证模块 422
安全设置/策略库 400
准入和禁入控制模块 410
访问隔离模块 430
创建的净盒/安全环境 440

图 4