(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 101483658 B
(45)授权公告日 2012.11.28

(21)申请号 200910104926.4

(22)申请日 2009.01.09

(73)专利权人 招商银行股份有限公司
地址 518040 广东省深圳市福田区深南大道7088号招商银行大厦十层

(72)发明人 熊少军 余仍辉 朱楠辉

(74)专利代理机构 深圳市凯达知识产权事务所 44256
代理人 王琦

(51)Int.Cl.
H04L 29/06(2006.01)
G06F 17/30(2006.01)

(56)对比文件
CN 101340281 A,2009.01.07,
CN 1983296 A,2007.06.20,
US 2004034794 A1,2004.02.19,
CN 101114323 A,2008.01.30,
KR 100710032 B1,2007.04.25,

审查员 李韧

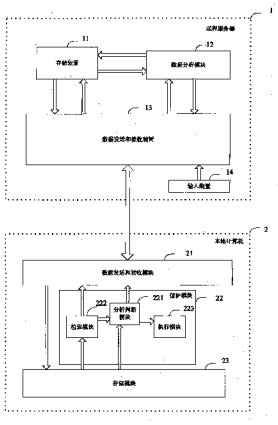
权利要求书 2 页 说明书 9 页 附图 6 页

(54)发明名称

浏览器输入内容保护的系统和方法

(57)摘要

本发明属于计算机网络安全技术领域，涉及一种浏览器输入内容保护的系统和方法，特别涉及一种WEB浏览器中输入的个人敏感信息保护的系统和方法。一种浏览器输入内容保护的系统，包括远程服务器和本地计算机，本地计算机设置有保护模块，所述的远程服务器设置有存储装置，该存储装置存储有配置数据，保护模块从远程服务器端下载配置数据，保护模块结合本地计算机中的钩子程序与配置数据中的恶意程序标识进行恶意程序识别，执行模块将识别出的恶意程序从钩子链表中删除。本法的保护系统和方法具有保护安全性高，对系统不产生影响，占用系统内存小的优点。



CN 101483658 B

1. 一种浏览器输入内容保护的系统，包括远程服务器和本地计算机，本地计算机设置有保护模块、数据发送和接收模块，所述的远程服务器设置有存储模块、数据发送和接收模块，存储模块中存储有配置数据，本地计算机从远程服务器端下载配置数据，保护模块结合下载的配置数据阻断恶意程序截获输入浏览器表单的数据；所述的配置数据信息包括钩子程序标识，所述的钩子程序标识包括恶意程序标识和非恶意程序标识。

2. 如权利要求 1 所述的一种浏览器输入内容保护的系统，其特征在于，所述的本地保护模块还包括检索模块、分析判断模块和执行模块，检索模块检测本地计算机中的钩子程序，分析判断模块结合本地计算机中的钩子程序与配置数据中的恶意程序标识进行恶意程序识别，执行模块阻断识别出的恶意程序截获用户输入浏览器表单的数据。

3. 如权利要求 2 所述的一种浏览器输入内容保护的系统，其特征在于，所述的配置数据中还包括受保护的网站信息，所述的分析判断模块分析用户浏览的网站信息，将此网站信息与配置数据中的受保护网站信息进行对比，检索模块在用户浏览受保护网站时检测本地计算机中的钩子程序，分析判断模块结合本地计算机中的钩子程序与配置数据中的恶意程序标识进行恶意程序识别，执行模块将识别出的恶意程序从钩子链表中删除。

4. 如权利要求 2 或 3 所述的一种浏览器输入内容保护的系统，其特征在于，所述的远程服务器还包括数据分析模块，保护模块中的检索模块检索本地计算机存储模块中的钩子程序，将该钩子程序发送给保护模块中的分析判断模块，分析判断模块结合配置数据中钩子程序标识确认未知的钩子程序，本地计算机中的数据接收和发送模块将未知的钩子程序发送到远程服务器，远程服务器的数据分析模块根据接收的未知的钩子程序通过数据分析模块进行数据分析，确认是否恶意，并将分析结果写入远程服务器的存储模块中。

5. 如权利要求 2 或 3 所述的一种浏览器输入内容保护的系统，其特征在于，所述的配置数据中还包含其版本信息，该版本信息包括该版本的版本号以及该版本的数据日期，所述的保护模块中的检索模块检索本地计算机存储模块中存储的配置数据的版本信息，并将这些版本信息通过本地计算机的数据发送模块发送给远程服务器，远程服务器中的数据接收模块接收到该版本信息之后，再通过远程服务器中的数据分析模块将该服务器中的配置数据的版本信息与本地计算机传送过来的版本信息进行比较，从而判断出该本地计算机需要更新的配置数据文件，并通过数据发送模块将需要升级的配置数据文件传送给该本地计算机。

6. 一种保护浏览器输入内容的方法，所述的浏览器安装在本地计算机上，本地计算机上还安装有一保护程序，其需要保护的输入内容被浏览器发送到远程服务器上，该方法包括以下步骤：

A. 下载保护程序，并安装，安装完成初始化；

B. 初始化完成后，保护程序从远程服务器上下载配置数据，所述的配置数据包括受保护的网站信息和钩子程序信息，下载完成后初始化；

C. 打开浏览器，自动加载保护程序；

D. 初始化完成后用户在浏览受保护网站的时候，保护程序结合受保护的网站信息启动保护，结合钩子程序信息中的恶意程序信息阻止钩子程序的运行。

7. 如权利要求 6 所述的保护浏览器输入内容的方法，其特征在于，所述的保护程序安装完成后，该保护程序作为一个浏览器辅助对象（Browser Helper Object）注册到浏览器

中。

8. 如权利要求6或7所述的保护浏览器输入内容的方法，其特征在于，所述的保护程序由用户主动下载源文件安装完成。

9. 如权利要求6或7所述的保护浏览器输入内容的方法，其特征在于，所述的保护程序由用户第一次浏览受保护的网站，经弹出窗口弹出，提示用户下载并安装。

10. 如权利要求9所述的保护浏览器输入内容的方法，其特征在于，所述的保护程序为一应用程序，其执行部分为一 ActiveX 控件。

11. 如权利要求6所述的保护浏览器输入内容的方法，其特征在于，所述步骤D进一步包括，保护程序启动保护后，保护程序检索本地计算机的电脑环境，结合配置数据中的钩子程序信息识别出未知的钩子程序，将未知的钩子程序信息发送到远程服务器中，远程服务器根据保护程序发送的钩子程序信息进行数据分析，确认程序是否恶意，并将这些钩子程序进行标识，将标识后的恶意程序信息和非恶意程序信息写入配置数据库中，并更新远程服务器中的配置数据库。

12. 如权利要求11所述的保护浏览器输入内容的方法，其特征在于，所述方法进一步包括，远程服务器向该本地计算机发送更新配置数据信息，该本地计算机根据该信息下载最新的配置数据，下载完成初始化，继续步骤D所述的过程。

13. 如权利要求6所述的保护浏览器输入内容的方法，其特征在于，所述步骤D中，用户在浏览网站的时候，保护程序根据配置数据中受保护网站信息与用户正在浏览的网站信息作出判断，如用户在浏览受保护的网站时，保护程序启动阻止钩子程序的运行；如用户在浏览不受保护的网站时，保护程序则忽略本地计算机中的钩子程序的运行。

14. 如权利要求6所述的一种保护浏览器输入内容的方法，其特征在于，在所述步骤D中，保护程序启动阻止钩子程序的运行时，保护程序检查计算机的电脑环境，检测本地计算机中存在的钩子程序，根据下载的配置数据信息确认存在于计算机中的钩子程序是否恶意，如果发现有能获取用户输入浏览器表单项内容的恶意程序，则将其从钩子表中删除，使其无法运行。

15. 如权利要求7所述的一种保护浏览器输入内容的方法，其特征在于，所述的配置数据中包括该配置数据的版本信息，该版本信息包括该版本的版本号以及该版本的数据日期信息，在步骤C的保护程序加载完成之后，保护程序与远程服务器建立起连接，向服务器发送本地计算机中的配置数据的版本信息，当本地计算机中配置数据版本比远程服务器中存储的配置数据版本要低时自动下载配置数据升级文件，完成更新后初始化保护程序，继续步骤D的过程。

浏览器输入内容保护的系统和方法

【技术领域】

[0001] 本发明属于计算机网络安全技术领域，涉及一种浏览器输入内容保护的系统和方法，特别涉及一种 WEB 浏览器中输入的个人敏感信息保护的系统和方法。

【背景技术】

[0002] 随着互联网的发展，基于 WEB 的应用日益普及，为各行业用户提供了超越时间和空间的服务通道，人们通过浏览器就可以完成包括查询银行账户、转账、电子商务等业务，为经济发展创造了良好条件，同时也为用户提供了方便、快捷的交互方式。但是，随着 WEB 应用的不断深入，需要在 WEB 上处理的个人敏感信息也越来越多，各种病毒、木马、恶意软件也盯上了人们在 WEB 上输入的敏感信息，并且已发展成为具备完整产业链的有组织犯罪团伙，给互联网安全带来了严重的问题，导致用户资金、身份被盗用，最终导致用户对网上银行、电子商务等不信任，严重阻碍了电子商务的发展。

[0003] 目前对浏览器输入内容的保护主要有以下几种保护密码的方法：

[0004] 1. 对浏览器中需要输入个人敏感信息的表单项的输入内容进行加密。例如，中国国家知识产权局专利数据库公开的动态密码的基运算加密法（公开号：CN1756152A，公开日：2006 年 4 月 5 日），服务器发出与客户密码相同位数的随机的附加码到客户端，客户用基运算加密法让真密码（静态密码，即原来的一般意义的密码）与附加码进行基运算得到动态密码作为为“假密码”返回服务器进行验证；还比如中国国家知识产权局专利数据库公开的 ActiveX 库的防止键盘记录编辑器（公开号：CN1547690，公开日：2004 年 11 月 17 日），该编辑器为一种具有 ActiveX 格式的用于 Web 浏览器和应用程序的安全程序，包括软件安全输入窗口，无需附加的硬连线装置而使用常规的键盘就可以防止泄露键盘数据。

[0005] 2. 结合辅助工具对信息输入者的合法性进行验证。例如中国国家知识产权局专利数据库公开了一种利用手持设备在一个连接过程中身份验证的方法（公开号：CN 1472915A，公开日：2004 年 2 月 4 日），服务器在连接过程中不断地要求客户端确认身份，客户端通过有线或无线连接与手持设备（如手机）通讯，获得身份验证；还比如中国国家知识产权局专利数据库公开的一种利用 USBkey 对网上银行数据进行认证的方法（公开号：CN 1556499A，公开日：2004 年 12 月 22 日），包括如下步骤：a) 根据用户信息生成针对该用产的数字证书；b) 将所述数字证书存入将要分配给该用户的 USB key 中；c) 用户登陆网上银行用户进行数据处理时，通过所述 USB key 确认用户身份或数字签名。

[0006] 3. 方法 1 和方法 2 的结合。

[0007] 上述几种防止网上银行密码被盗的方式只是一个被动式的防御过程，通过不断的加载密码转换工具和密码筛选验证工具来弥补安全漏洞，其只能对客户输入的网上银行密码内容进行保护，无法对其他的个人敏感信息内容进行保护，因为客户在申请注册网上银行的时候需要在网站上填写很多个人私密信息，而客户设定的网上银行密码很可能与这些私密信息相关，有些黑客人员通过这些私密信息就可以推断出客户的密码。不仅仅客户的密码与这些私密信息相关，其验证密码合法性的辅助工具也与这些私密信息相关，例如用

户的手机号码，USB key 验证信息等。

[0008] 所以不仅保护用户网上银行的密码重要，保护用户的个人敏感信息同样重要。

[0009] 另一方面，上述几种保护网上银行密码的方式不能从根本上解决网上银行账户和密码被盗的问题，由于微软的 windows 操作系统是建立在事件驱动的机制上的，也就是通过消息传递来实现。而钩子在 windows 操作系统中，是一种能在事件（比如：消息、鼠标激活、键盘响应）到达应用程序前中途接获事件的机制。所以钩子就作为一个能被非法程序利用的后门，每一个 Hook（钩子）都有一个与之相关联的指针列表，称之为钩子链表，由系统来维护。这个列表的指针指向指定的，应用程序定义的，被 Hook 子程调用的回调函数，也就是该钩子的各个处理子程。当与指定的 Hook 类型关联的消息发生时，系统就把这个消息传递到 Hook 子程。一些 Hook 子程可以只监视消息，或者修改消息，或者停止消息的前进，避免这些消息传递到下一个 Hook 子程或者目的窗口。最近安装的钩子放在链的开始，而最早安装的钩子放在最后，也就是后加入的先获得控制权。

[0010] 木马程序是一种典型的恶意程序，木马程序可以通过钩子注入方式将自身的模块加载到正常进程中。在这种情况下，由于木马程序的模块运行的上下文是当前进程空间，因而只要当前进程是可信的，木马程序的任何动作也都是可信的。这样，木马程序就可以在可信的正常进程庇护下窃取用户的信息。

[0011] 所以即使采用了对键盘加密的程序以及增加用户合法性的验证项，只要恶意程序利用了钩子 (Hook) 并在系统中运行，都有可能将用户的个人敏感信息盗取。

[0012] 【发明内容】

[0013] 本发明为了从根本上解决网上银行个人敏感信息被盗取，防止用户在网上银行或者其他需要保护的网站丢失敏感信息导致的资金损失。

[0014] 本发明采取的技术方案如下：

[0015] 一种浏览器输入内容保护的系统，包括远程服务器和本地计算机，本地计算机设置有保护模块，所述的远程服务器设置有存储装置，该存储装置存储有配置数据，保护模块从远程服务器端下载配置数据，保护模块结合下载的配置数据阻断恶意程序截获输入浏览器表单的数据。

[0016] 所述的恶意程序包括木马、病毒以及其他广告程序等。

[0017] 本地保护模块可以将远程服务器中的配置数据下载到本地计算机的虚拟内存或者内存中，也可以存储在本地计算机中的磁盘中，由于存储在本地计算机中的磁盘中在重启计算机后无需重新下载配置数据，所述的计算机的磁盘即为存储模块，所以进一步的，所述的本地计算机还包括存储模块，所述的本地计算机从远程服务器下载配置数据存储在本地存储模块中。

[0018] 钩子程序包括恶意程序和非恶意程序。

[0019] 所述的配置数据信息包括受保护的网站信息、钩子程序标识，所述的钩子程序标识包括恶意程序标识和非恶意程序标识。

[0020] 所述的本地保护模块还包括检索模块、分析判断模块和执行模块，检索模块检测本地计算机中的钩子程序，分析判断模块结合本地计算机中的钩子程序与配置数据中的恶意程序标识进行恶意程序识别，执行模块阻断识别出的恶意程序截获用户输入浏览器表单的数据。

[0021] 阻断恶意程序截获用户输入浏览器表单的数据可以有很多方法，一种方法是直接删除或者卸载恶意程序，一种方法直接使恶意程序停止运行，比如删除恶意程序在钩子链表中的数据。

[0022] 进一步的，所述的配置数据中还包括受保护的网站信息，所述的分析判断模块分析用户浏览的网站信息，将此网站信息与配置数据中的受保护网站信息进行对比，检索模块在用户浏览受保护网站时检测本地计算机中的钩子程序，分析判断模块结合本地计算机中的钩子程序与配置数据中的恶意程序标识进行恶意程序识别，执行模块将识别出的恶意程序从钩子链表中删除。

[0023] 所述的远程服务器还包括数据分析模块。

[0024] 保护模块中的检索模块检索本地计算机存储模块中的钩子程序，将该钩子程序发送给保护模块中的分析判断模块，分析判断模块结合配置数据中钩子程序标识确认未知的钩子程序，本地计算机中的数据发送模块将未知的钩子程序发送到远程服务器，远程服务器的数据分析模块根据接收的未知的钩子程序通过数据分析模块进行数据分析，确认是否恶意，并将分析结果写入远程服务器的存储装置中。

[0025] 所述的配置数据中还包含其版本信息，该版本信息包括该版本的版本号以及该版本的数据日期，所述的保护模块中的检索模块检索本地计算机存储模块中存储的配置数据的版本信息，并将这些版本信息通过本地计算机的数据发送模块发送给远程服务器，远程服务器中的数据接收模块接收到该版本信息之后，再通过远程服务器中的数据分析模块将该服务器中的配置数据的版本信息与本地计算机传送过来的版本信息进行比较，从而判断出该本地计算机需要更新的配置数据文件，并通过数据发送模块将需要升级的配置数据文件传送给该本地计算机。

[0026] 所述的本地保护模块作为一个浏览器辅助对象(Browser Helper Object)注册到浏览器中。

[0027] 所述的保护模块为一保护程序的子程序，该保护程序的安装源文件存储在远程服务器中。该保护程序的安装源文件也可以存储在各个下载服务器中，供用户自由的下载。

[0028] 所述的保护程序的源程序为一应用程序，其执行部分为一 ActiveX 控件。

[0029] 用户需要安装该 ActiveX 控件可以主动去下载服务器中找到下载链接下载，也可以被动由某一装置提示被动下载。因此，进一步的，所述的本地计算机还包括下载 ActiveX 控件的弹出模块，该弹出模块包含一弹出窗口，该弹出窗口在用户第一次访问受保护网站时被弹出模块调用出来。

[0030] 本发明还提供了一种保护浏览器输入内容的方法，所述的浏览器安装在本地计算机上，本地计算机上还安装有一保护程序，其需要保护的输入内容被浏览器发送到远程服务器上，该方法包括以下步骤：

[0031] A. 下载保护程序，并安装，安装完成初始化；

[0032] B. 初始化完成后，保护程序从远程服务器上下载配置数据，所述的配置数据包括受保护的网站信息和钩子程序信息，下载完成后初始化；

[0033] C. 打开浏览器，自动加载保护程序；

[0034] D. 初始化完成后用户在浏览受保护网站的时候，保护程序结合受保护的网站信息启动保护，结合钩子程序信息中的恶意程序信息阻止钩子程序的运行。

[0035] 所述的保护程序安装完成后，该保护程序作为一个浏览器辅助对象 (Browser Helper Object) 注册到浏览器中。

[0036] 所述的保护程序由用户主动下载源文件安装完成。

[0037] 所述的保护程序也可由用户第一次浏览受保护的网站，经弹出窗口弹出，提示用户下载并安装。

[0038] 所述的保护程序为一应用程序，其执行部分为一 ActiveX 控件。

[0039] 所述步骤 D 进一步包括，保护程序启动保护后，保护程序检索本地计算机的电脑环境，结合配置数据中的钩子程序信息识别出未知的钩子程序，将未知的钩子程序信息发送到远程服务器中，远程服务器根据保护程序发送的钩子程序信息进行数据分析，确认程序是否恶意，并将这些钩子程序进行标识，将标识后的恶意程序信息和非恶意程序信息写入配置数据库中，并更新远程服务器中的配置数据库。

[0040] 所述方法进一步包括，远程服务器向该本地计算机发送更新配置数据信息，该本地计算机根据该信息下载最新的配置数据，下载完成初始化，继续步骤 D 所述的过程。

[0041] 所述步骤 D 中，用户在浏览网站的时候，保护程序根据配置数据中受保护网站信息与用户正在浏览的网站信息作出判断，如用户在浏览受保护的网站时，保护程序启动阻止钩子程序的运行。如用户在浏览不受保护的网站时，保护程序则忽略本地计算机中的钩子程序的运行。

[0042] 在所述步骤 D 中，保护程序启动阻止钩子程序的运行时，保护程序检查计算机的电脑环境，检测本地计算机中存在的钩子程序，根据下载的配置数据信息确认存在于计算机中的钩子程序是否恶意，如果发现有能获取用户输入浏览器表单项内容的恶意程序，则将其从钩子表中删除，使其无法运行。

[0043] 如钩子程序为非恶意程序，则保护程序不将其从钩子表中删除。

[0044] 所述的配置数据中包括该配置数据的版本信息，该版本信息包括该版本的版本号以及该版本的数据日期信息，在步骤 C 的保护程序加载完成之后，保护程序与远程服务器建立起连接，向服务器发送本地计算机中的配置数据的版本信息，当本地计算机中配置数据版本比远程服务器中存储的配置数据版本要低时自动下载配置数据升级文件，完成更新后初始化保护程序，继续步骤 D 的过程。

[0045] 为了使保护程序能够正常的运行，需要通过保护程序启动系统的禁止远程执行等功能。

[0046] 本发明的有益效果在于：

[0047] 1. 由于保护程序在启动保护的过程中，只在钩子链表中删除恶意的钩子程序，使钩子程序无法在内存中运行，从而无法截获用户个人信息，在此过程中，不删除病毒或木马，不会产生误删系统文件的可能，保证了系统的长期稳定。

[0048] 2. 由于不同的网站鉴别钩子程序是否为恶意非常困难，所以保护程序只在用户浏览受保护的网站时才开启，保证了用户在浏览其他的网站时能正常运行，占用系统内存小。

[0049] 3. 本发明能不仅能有效的保护用户的密码信息，还能从根本上全面保护用户输入到浏览器表单项的个人敏感信息。

[0050] 4. 由于保护程序只在用户第一次登陆受保护的网站需要下载配置数据，初始化完成用户或者在以后的浏览器登陆中，保护程序自动根据下载的配置数据和本地计算机电脑

环境作出执行删除钩子表中的恶意程序的工作，整个过程不影响用户使用时的浏览网页的速度。

[0051] 5. 本发明的保护程序可以和之前的程序相兼容，不会强制用户下载并安装使用。

【附图说明】

[0052] 图 1 为本发明的浏览器输入内容保护系统的结构框图；

[0053] 图 2 为本发明的配置数据的示意图；

[0054] 图 3 为本发明的保护浏览器输入内容的方法中的方法一的流程图；

[0055] 图 4 为本发明的保护浏览器输入内容的方法中的方法二的流程图；

[0056] 图 5 为本发明的保护浏览器输入内容的方法中的方法三的流程图；

[0057] 图 6 为本发明的保护浏览器输入内容的方法中的方法四的流程图；

【具体实施方式】

[0058] 如图 1，图 2 所示，本发明提供了一种浏览器输入内容保护系统，该系统包括远程服务器 1 和本地计算机 2，远程服务器 1 和本地计算机 2 通过万维网相连，一个远程服务器 1 和多个本地计算机 2 互通数据。远程服务器 1 包括存储装置 11、数据分析模块 12、数据发送和接收装置 13。该存储装置 11 上存储有配置数据库 3，所述的配置数据库 3 中的配置数据 31 包括受保护的网站信息 332 和钩子程序信息 333，受保护的网站 332 主要是指那些需要在上面填写个人真实信息的网站，而这些个人真实信息中还包含有涉及到个人生命或者财产安全的信息，例如银行网站以及其他电子商务网站。钩子程序包括键盘钩子、鼠标钩子、消息钩子、外壳钩子、日志钩子、窗口钩子以及全局钩子。有些钩子程序会被恶意程序利用，例如键盘钩子，木马程序通过调用全局钩子来捕获任意窗口的键盘输入。在钩子程序信息 333 中标识出恶意程序 3331 和非恶意程序 3332 就可以很好的找出本地计算机中存在的潜在威胁。本地计算机 2 中安装有操作系统和浏览器，浏览器可以通过 TCP/IP 协议自由的访问互联网，同时本地计算机 2 还安装有保护程序，该保护程序实质上一个本地计算机硬件的一个调用程序，本地计算机硬件包括内存、CPU、显卡、网卡、磁盘以及承载这些硬件的主板，我们可以将该保护程序分割为保护模块 22、存储模块 23、数据发送和接收模块 21，本地计算机 2 中的数据发送和接收模块 21 发送下载配置数据 31 的指令到远程服务器 1，远程服务器 1 中的数据发送和接收装置 13 将配置数据 31 通过互联网打包传送给本地计算机 2，本地计算机 2 中的数据发送和接收模块 21 接收配置数据 31，并通过其存储模块 23 存储在本地计算机的中，以供本地计算机的保护模块 22 随时调用。保护模块 22 包括检索模块 222、分析判断模块 221 和执行模块 223，检索模块 222 检测本地计算机 2 中存在的钩子程序，并将这些钩子程序发送给分析判断模块 221，分析判断模块 221 结合配置数据中的恶意程序标识 3331 确认本地计算机 2 中的恶意程序，执行模块 223 将恶意的钩子程序从钩子链表中删除，钩子程序从钩子链表中删除后，程序则无法在内存中运行，因而无法截获用户输入信息。

[0059] 远程服务器 1 中的存储模块 11 中存储的配置数据中的受保护的网站信息 332 由远程服务器 1 端的输入模块 14 来添加、删除或者修改。随着互联网技术的不断发展，更多的钩子程序会被技术人员开发出来，同时也会有更多的钩子程序被恶意程序利用，所以需

要常常更新远程服务器 1 中的配置数据才能更好的对需要受保护的网站实行保护。

[0060] 通过保护模块 22 中的检索模块 222 来检测本地计算机 2 中的钩子程序，这些钩子程序中包括恶意程序和非恶意程序，将这些钩子程序发送给保护模块 22 中的分析判断模块 221，分析判断模块 221 结合存储在本地计算机 2 中的配置数据进行比较，如发现本地计算机 2 中的存在的钩子程序未在配置数据中进行标识后，则保护模块 22 的分析判断模块 221 将未知的钩子程序通过本地计算机 2 的数据发送和接收模块 21 发送给远程服务器 1，远程服务器 1 中的数据发送和接收装置 13 将接收到未知的钩子程序交给远程服务器中的数据分析模块 12 进行数据分析，确认程序是否为恶意程序，如为恶意程序，则将这些恶意的钩子程序进行恶意程序标识 3331，如为非恶意程序，则将这些非恶意的钩子程序进行非恶意程序标识 3332，数据分析模块 12 将这些标识的未知的钩子程序存储在存储装置 11 中，并更新配置数据 31。在有的时候，一种新的恶意程序的出现会在很短的时间在互联网中传播开来，本地计算机 2 一旦没有更新配置数据 31，分析判断模块 221 则不会识别出本地计算机 2 中存在的恶意的钩子程序，则不会通过执行模块 223 去删除钩子链表中的该恶意程序，不能起到保护的作用，所以必须使本地计算机 2 及时更新配置数据 31。

[0061] 远程服务器 1 通过数据发送和接收装置 13 将配置数据 31 已经更新的信息发送给本地计算机 2，本地计算机 2 会根据其更新信息下载更新的配置数据 31 文件，以升级本地的配置数据 31 文件。在这里面会出现一个问题，那就是远程服务器 1 无法向互联网中的全部本地计算机 2 发送更新信息，因为不是所有本地计算机 2 中的配置数据 31 都是一样的，而且本地计算机 2 也不是每个都同时开了浏览器的，因此，在每个本地计算机 2 的配置数据库 31 中标识此配置数据的版本信息 331，该版本信息 331 包括该版本的版本号 3311 以及该版本的日期 3312，在本地计算机 2 打开浏览器后，本地计算机 2 中的检索模块 222 检索该计算机存储模块 23 中存储的配置数据的版本信息 331，并将这些版本信息 331 通过本地计算机 2 的数据发送和接收模块 21 发送给远程服务器 1 后，远程服务器 1 中的数据发送和接收装置 13 接收到此信息之后，再通过远程服务器 1 中的数据分析模块 12 将该服务器 1 中的配置数据的版本信息 331 与本地计算机传送过来的版本信息 331 进行比较，从而判断出该本地计算机需要更新的配置数据文件，并通过数据发送和接收装置 13 将需要升级的配置数据文件传送给该本地计算机。

[0062] 由于远程服务器 1 中的配置数据 31 根据互联网的环境需要进行了不断的升级，所以需要本地计算机 2 在每次启动浏览器后即自动连接远程服务器 1 以检查本地计算机 2 中的配置数据 31 是否为最新，如果本地计算机 2 中的配置数据 31 已经为最新则无须升级。

[0063] 下面就本发明提供的一种保护浏览器输入内容的方法作进一步说明，一种保护浏览器输入内容的方法，所述的浏览器安装在操作系统中，所述的操作系统不仅仅指目前的 windows 操作系统，还包括开源代码的操作系统，包括 Linux、Mac 操作系统，这些操作系统被安装在本地计算机（用户计算机）中，多个本地计算机（用户计算机）与一个远程服务器通过 Internet 互通数据。该方法是这样实现的：

[0064] 方法一，如图 3 所示：

[0065] 1. 在用户使用本发明所述的保护系统之前需要下载一保护程序并安装，该保护程序是一个应用程序，其执行部分为一个 ActiveX 控件，保护程序的源程序存储在远程服务器中，用户在第一次浏览受保护的网站时，会出现一个弹出窗口，提示用户安装 ActiveX

控件，用户安装完成保护程序后，保护程序在浏览器中注册为辅助浏览器对象 (Browser Helper Object)，并将辅助浏览器对象 (Browser Helper Object) 信息写入注册表 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects 的 CLSID 中，安装完成后保护程序初始化；

[0066] 2. 步骤 1 中的初始化完成后，保护程序自动加载；

[0067] 3. 步骤 2 中的加载完成之后，保护程序自动从远程服务器中下载配置数据，下载完成后保护程序根据配置数据信息进行初始化；

[0068] 4. 步骤 3 中的初始化完成之后，保护程序检查用户电脑环境，检测本地计算机中存在的钩子程序，根据下载的配置数据，保护程序确认本地计算机中存在的恶意程序，这些恶意程序有可能获取用户输入到浏览器表单中内容的信息，保护程序将其中钩子链表中删除。在此过程中只使恶意程序无法运行，不直接删除恶意程序；

[0069] 5. 在步骤 4 中在保护程序检测本地计算机中存在的钩子程序时必定会出现一种情况，那就是本地计算机中存在配置数据中没有出现的钩子程序，这些钩子程序是否为恶意程序，没有经过分析无从得知，而本地计算机的保护程序没有分析钩子程序的危险级别的功能，所以需要将此未知的钩子程序发送给远程服务器进行分析。所以此过程为：保护程序将未知的钩子程序发送给远程服务器，远程服务器根据保护程序发送的未知的钩子程序信息进行数据分析，确认该未知的钩子程序是否为恶意程序，并将该未知钩子程序进行标识，并将该标识信息存入配置数据库中，完成存储后服务器更新配置版本信息，远程服务器将配置更新的信息发送给该本地计算机，该本地计算机根据该信息下载最新的配置数据，下载完成初始化，继续步骤 4 所述的过程。

[0070] 上述方法一是用户在没有安装保护程序并且第一次浏览受保护网站的时候实现的过程，当用户在安装完成保护程序后再次浏览受保护的网站的时候是通过下述的方法二实现的。

[0071] 方法二，如图 4 所示：

[0072] 1. 用户启动浏览器时，自动加载保护程序；

[0073] 2. 在步骤 1 中的保护程序加载完成之后，保护程序与远程服务器建立起连接，向远程服务器发送本地计算机中的配置数据的版本信息，当本地计算机中配置数据版本比远程服务器中存储的配置数据版本要低时自动下载配置数据升级文件，完成更新后初始化保护程序。如果检测到本地计算机中的配置数据已经是最新时，则将信息返回给保护程序，无需下载，直接进入下一步；

[0074] 3. 在步骤 3 中的保护程序初始化完成后，保护程序检查用户电脑环境，检测本地计算机中存在的钩子程序，根据下载的配置数据，保护程序确认本地计算机中存在的恶意程序，这些恶意程序有可能获取用户输入到浏览器表单中内容的信息，保护程序将其中钩子链表中删除。在此过程中只使恶意程序无法运行，不直接删除恶意程序；

[0075] 4. 在步骤 3 中将保护程序检测到的未知的钩子程序发送给远程服务器进行分析，远程服务器根据保护程序发送的未知的钩子程序信息进行数据分析，确认该未知的钩子程序是否为恶意程序，并将该未知钩子程序进行标识，并将该标识信息存在在配置数据中，完成存储后服务器更新配置版本信息，远程服务器将配置更新的信息发送给本地计算机，本地计算机根据该信息下载最新的配置数据，下载完成初始化，继续步骤 3 所述的过程。

[0076] 上述方法二是在用户在安装完成保护程序后再次浏览受保护网站的时候实现的过程。当用户在其他网站下载保护程序的安装源程序安装，安装完成保护程序后第一次浏览不受保护网站的时候是通过下述的方法三实现的。

[0077] 方法三，如图 5 所示：

[0078] 1. 用户从合作网站主动下载保护程序的源文件，并安装，用户安装完成保护程序后，保护程序在浏览器中注册为辅助浏览器对象 (Browser Helper Object)，并将辅助浏览器对象 (Browser Helper Object) 信息写入注册表 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects 的 CLSID 中，安装完成后保护程序初始化；

[0079] 2. 启动浏览器时，自动加载保护程序；

[0080] 3. 步骤 2 中的加载完成之后，保护程序自动从远程服务器中下载配置数据，下载完成后保护程序根据配置数据信息进行初始化，初始化完成后的步骤和方法一的步骤 4，5 相同；

[0081] 4. 步骤 3 完成之后，保护程序根据用户打开浏览器的网站判断其浏览的是否为受保护的网站，

[0082] 5. 当用户浏览受保护的网站时，执行与方法一中的步骤 4，5 相同的过程；用户浏览不受保护的网站时，步骤 3 中初始化完成之后，保护程序不工作。

[0083] 上述方法三是当用户在其他网站下载保护程序的安装源程序安装，安装完成保护程序后第一次浏览网站时候的实现过程，当用户在其他网站下载保护程序的安装源程序安装，安装完成保护程序后再次浏览网站的时候，是通过下述方法四实现的。

[0084] 方法四，如图 6 所示：

[0085] 1. 用户从合作网站主动下载保护程序的源文件，并安装，用户安装完成保护程序后，保护程序在浏览器中注册为辅助浏览器对象 (Browser Helper Object)，并将辅助浏览器对象 (Browser Helper Object) 信息写入注册表 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects 的 CLSID 中，安装完成后保护程序初始化；

[0086] 2. 用户启动浏览器时，自动加载保护程序；

[0087] 3. 在步骤 1 中的保护程序加载完成之后，保护程序与远程服务器建立起连接，向服务器发送本地计算机中的配置数据的版本信息，当本地计算机中配置数据版本比远程服务器中存储的配置数据版本要低时自动下载配置数据升级文件，完成更新后初始化保护程序。如果检测到本地计算机中的配置数据已经是最新时，则将信息返回给保护程序，无需下载，直接进入下一步；

[0088] 4. 保护程序判断浏览的网站是否为受保护的网站，用户浏览不受保护的网站时，步骤 3 中初始化完成之后，保护程序不工作；用户浏览受保护的网站时，继续完成与方法一中的步骤 4，5 相同的过程。

[0089] 本发明给出的上述四种方法虽然不能全面的概括用户在使用的过程中出现的各种情况的实现过程，但是普通的技术人员通过上述四种方法再加上简单的推理就可以实现用户在各种情况下的实现过程。

[0090] 同时需要说明的是在上述具体实施方式中虽然给出了本发明浏览器输入内容保

护方法的自动实现的过程，但是在实际运用时，为了尊重用户的使用习惯，在各步骤中的下载安装过程可以提醒用户手动完成，所以可以增加弹出窗口来实现上述的提醒过程，这些普通的技术人员利用目前的技术就可以实现，所以虽然本发明没有进一步给出弹出窗口的提示过程，但是这并不影响本专利的保护范围。

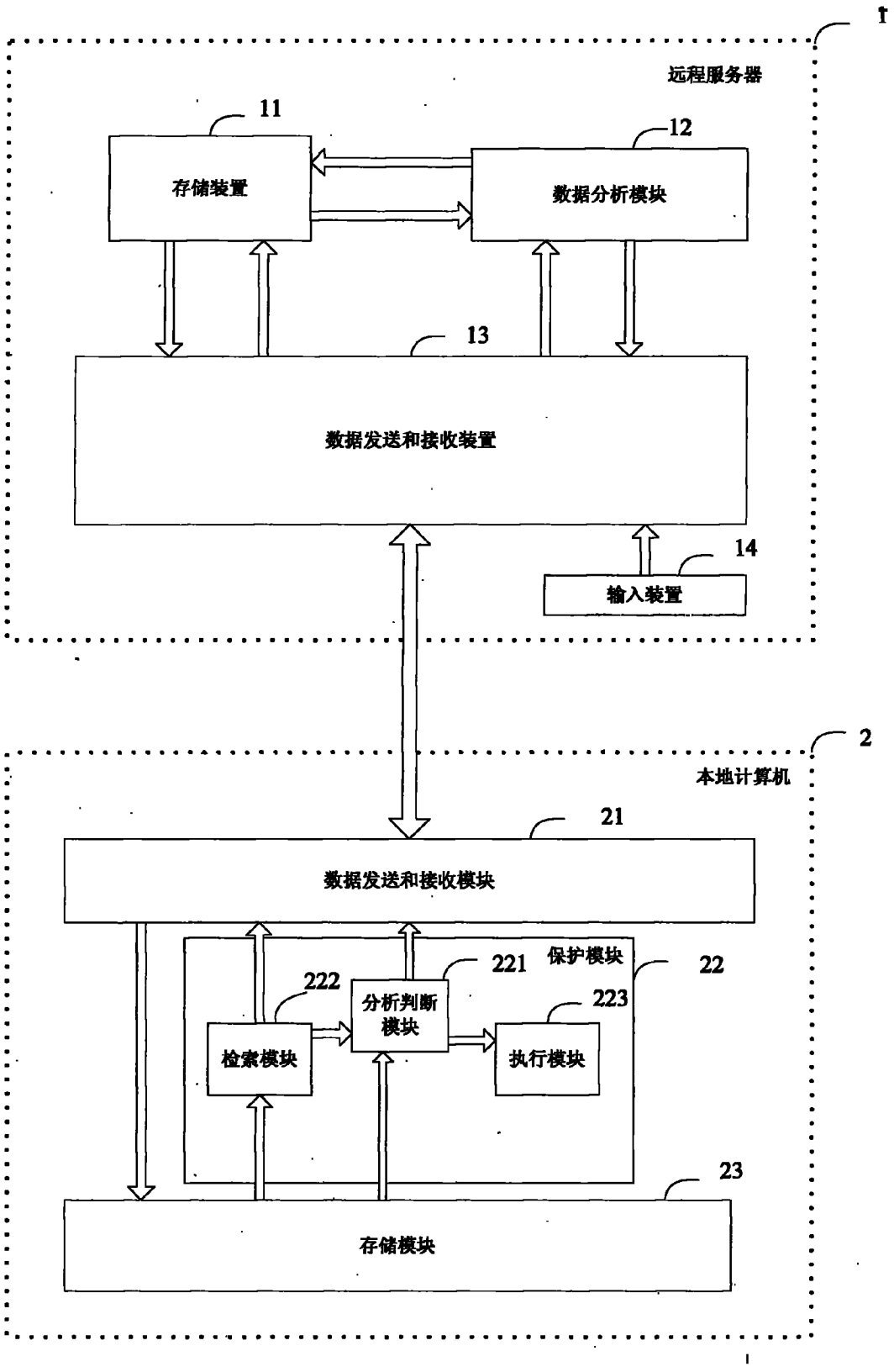

1
远程服务器
11
存储装置
12
数据分析模块
13
数据发送和接收装置
14
输入装置
2
本地计算机
21
数据发送和接收模块
保护模块
22
221
222
分析判断模块
223
检索模块
执行模块
23
存储模块

图 1

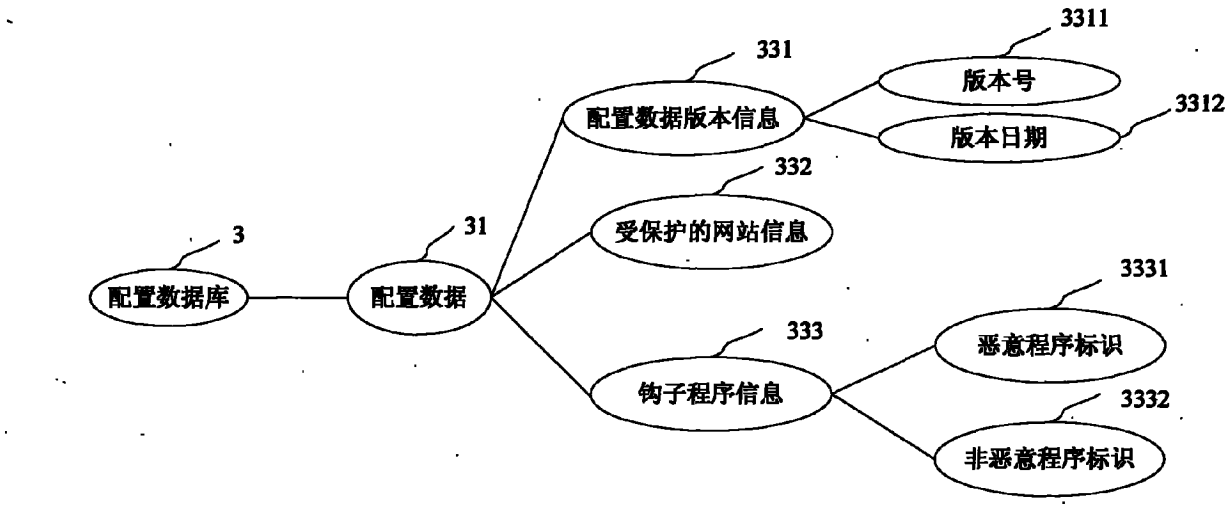

3
配置数据库
31
配置数据
331
配置数据版本信息
3311
版本号
3312
版本日期
332
受保护的网站信息
333
钩子程序信息
3331
恶意程序标识
3332
非恶意程序标识

图 2

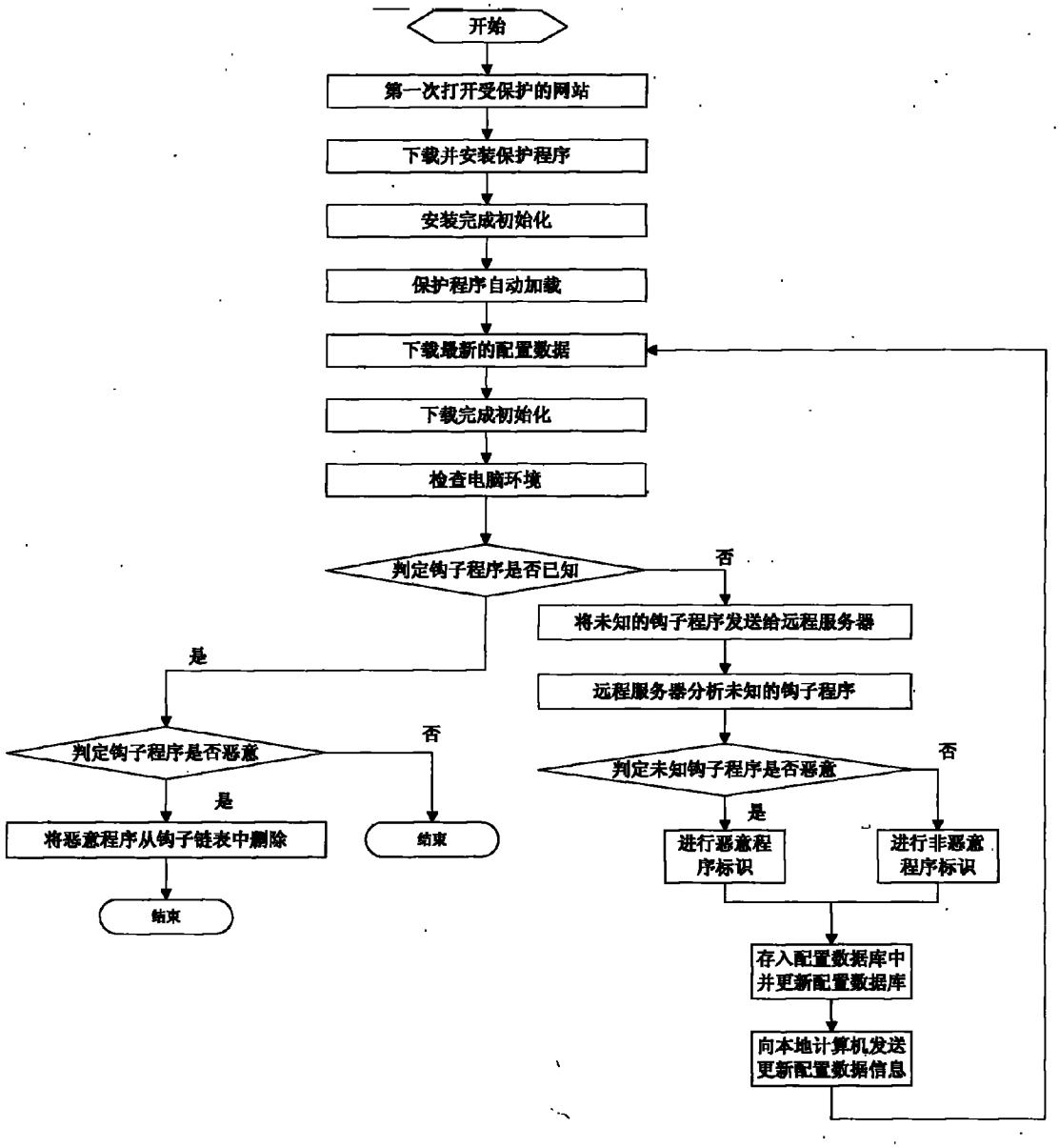

开始
第一次打开受保护的网站
下载并安装保护程序
安装完成初始化
保护程序自动加载
下载最新的配置数据
下载完成初始化
检查电脑环境
判定钩子程序是否已知
否
是
将未知的钩子程序发送给远程服务器
远程服务器分析未知的钩子程序
判定钩子程序是否恶意
否
是
判定未知钩子程序是否恶意
否
是
将恶意程序从钩子链表中删除
结束
进行恶意程序标识
进行非恶意程序标识
结束
存入配置数据库中并更新配置数据库
向本地计算机发送更新配置数据信息

图 3

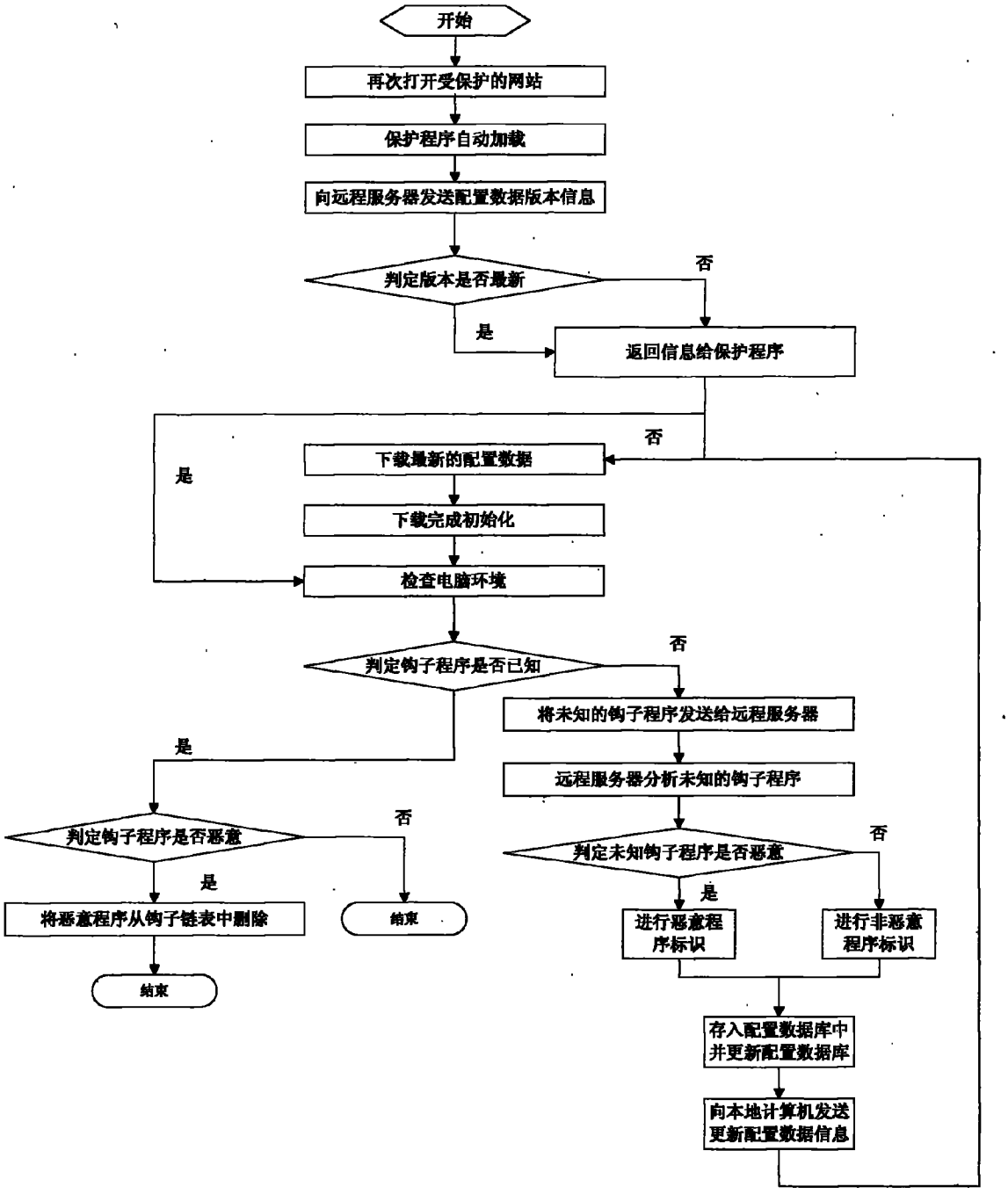

开始
再次打开受保护的网站
保护程序自动加载
向远程服务器发送配置数据版本信息
判定版本是否最新
否
是
返回信息给保护程序
否
是
下载最新的配置数据
下载完成初始化
检查电脑环境
判定钩子程序是否已知
否
将未知的钩子程序发送给远程服务器
是
远程服务器分析未知的钩子程序
判定钩子程序是否恶意
否
判定未知钩子程序是否恶意
否
是
是
将恶意程序从钩子链表中删除
结束
进行恶意程序标识
进行非恶意程序标识
结束
存入配置数据库中并更新配置数据库
向本地计算机发送更新配置数据信息

图 4

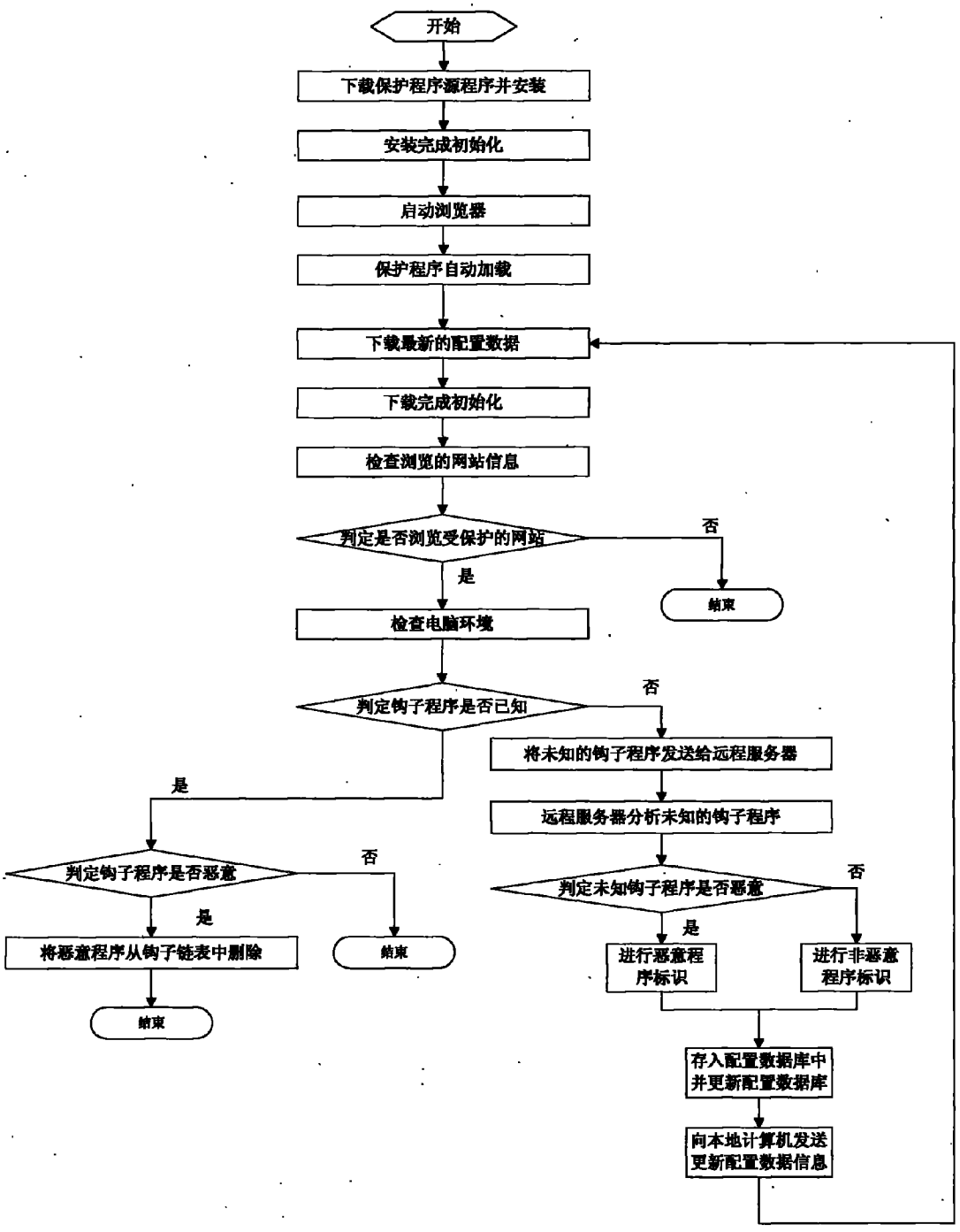

开始
下载保护程序源程序并安装
安装完成初始化
启动浏览器
保护程序自动加载
下载最新的配置数据
下载完成初始化
检查浏览的网站信息
判定是否浏览受保护的网站
否
结束
是
检查电脑环境
判定钩子程序是否已知
否
将未知的钩子程序发送给远程服务器
是
远程服务器分析未知的钩子程序
判定钩子程序是否恶意
否
判定未知钩子程序是否恶意
否
是
将恶意程序从钩子链表中删除
结束
是
进行恶意程序标识
进行非恶意程序标识
结束
存入配置数据库中并更新配置数据库
向本地计算机发送更新配置数据信息

图 5

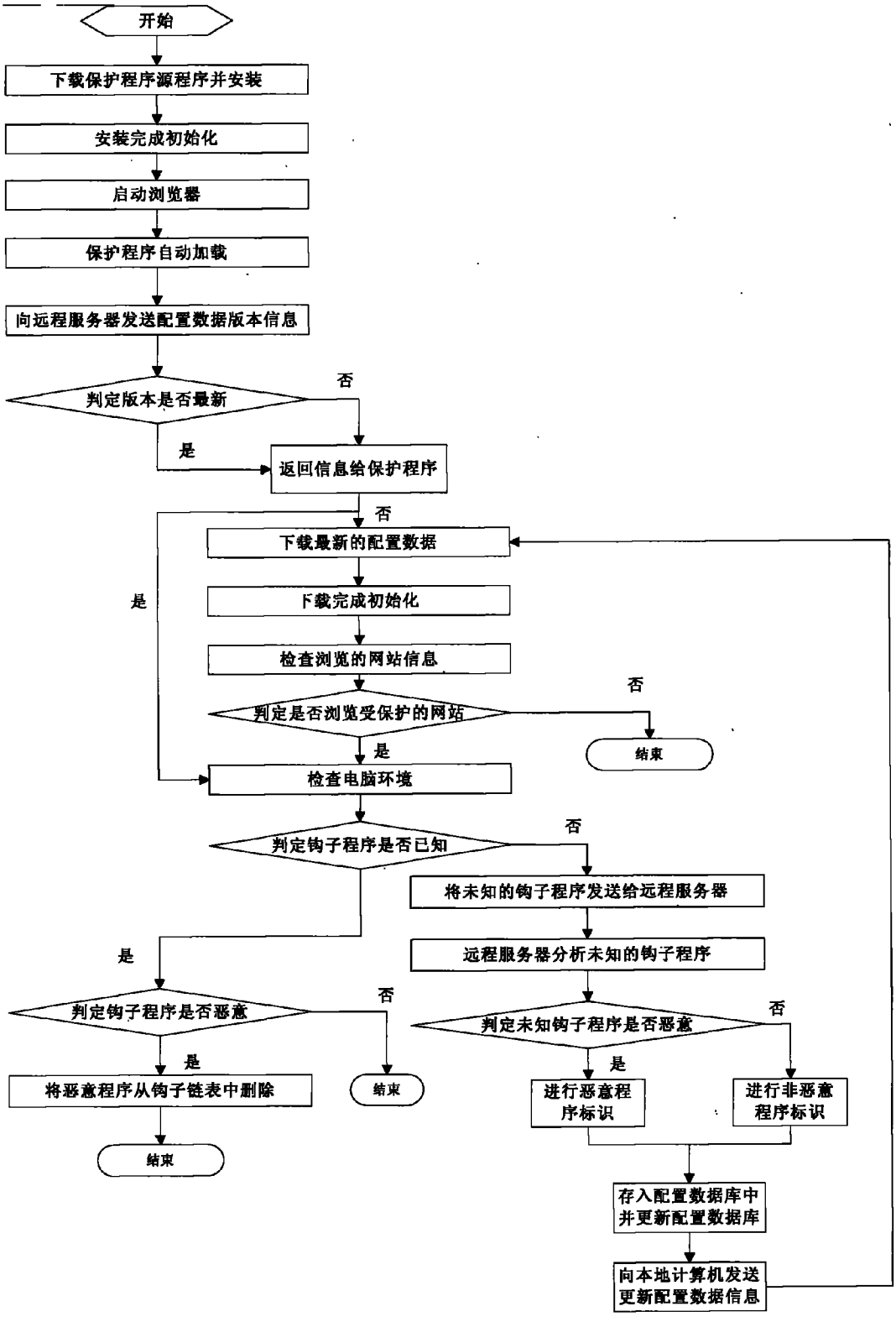

开始
下载保护程序源程序并安装
安装完成初始化
启动浏览器
保护程序自动加载
向远程服务器发送配置数据版本信息
判定版本是否最新
否
是
返回信息给保护程序
否
下载最新的配置数据
是
下载完成初始化
检查浏览的网站信息
判定是否浏览受保护的网站
否
结束
是
检查电脑环境
判定钩子程序是否已知
否
将未知的钩子程序发送给远程服务器
远程服务器分析未知的钩子程序
是
判定钩子程序是否恶意
否
判定未知钩子程序是否恶意
否
是
将恶意程序从钩子链表中删除
结束
是
进行恶意程序标识
进行非恶意程序标识
结束
存入配置数据库中并更新配置数据库
向本地计算机发送更新配置数据信息

图 6