[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200610078622.1

[43] 公开日 2007 年 1 月 24 日

[11] 公开号 CN 1900941A

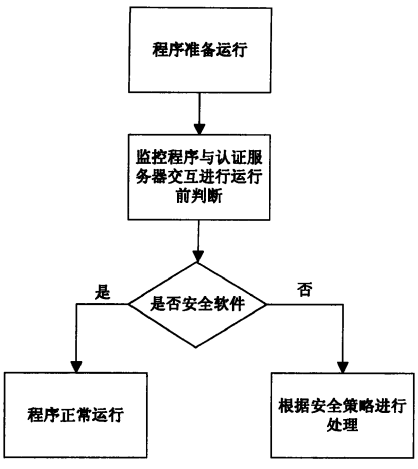
[22] 申请日 2006.4.28
[21] 申请号 200610078622.1
[71] 申请人 傅玉生
地址 100021 北京市朝阳区西大望路 59 号 7 号楼 2 单元 201
[72] 发明人 傅玉生
权利要求书 1 页 说明书 5 页 附图 3 页

[54] 发明名称

一种基于软件身份认证技术的计算机安全保护方法

[57] 摘要

本发明涉及计算机安全领域，基于软件身份认证的思路，建立以认证服务器为中心的客户端计算机安全保护机制。 本发明的内容包括：1. 以可执行文件的唯一特征码为标识，建立安全认证数据库；2. 以安全认证数据库为核心，建立提供软件安全认证功能的认证服务器；3. 制定限制客户端软件运行的安全策略；4. 监控客户端计算机，在可执行文件启动前提取其唯一特征码，并提交给认证服务器；5. 认证服务器查询安全认证数据库，将相应的安全信息反馈给客户端计算机；6. 客户端计算机根据反馈的信息和预定的策略，判断是否执行该软件。 本发明利用但不唯一依赖于对有害程序特征码的识别，相比传统防病毒方法，具有更广泛的保护能力，可有效切断有害程序的执行途径。



1. 一种以软件身份识别为基础，采用安全认证数据库和认证服务器对软件进行集中认证的计算机系统安全保护方法，使用这种方法建立一个只允许已知可信的安全软件运行的计算机系统环境。

2. 根据权利要求 1 所述的方法，其特征在于：安全认证数据库是存储软件的特征信息和安全信息的数据库，数据库中存储的软件都利用可执行文件的唯一特征码进行标识。

3. 根据权利要求 1 所述的方法，其特征在于：软件的安全由认证服务器进行认证；认证的根据是可执行文件的唯一特征码；认证服务器根据唯一特征码从安全认证数据库中搜索出该软件的安全信息和特征信息，并把这些信息反馈给客户端监控程序。

4. 根据权利要求 1 所述的方法，其特征在于：实施的过程由四个环节构成（1）建立安全认证数据库；（2）建立并运行认证服务器；（3）设计允许软件运行的安全策略；（4）安装并运行监控程序。

5. 根据权利要求 1 所述的方法，其特征在于：采用的可执行文件的唯一特征码是该文件的统计特征，是将文件所包含的连续二进制序列作为输入数据，经过预定的算法计算所获得的具有唯一确定性的数据形式记录。

6. 根据权利要求 1 所述的方法，其特征在于：获得可执行文件唯一特征码的算法为散列算法，例如 MD4，MD5，SHA。

7. 根据权利要求 1 所述的方法，其特征在于：安全认证数据库中的软件特征信息包括软件的名称，厂商，版本，软件可执行文件名称，软件的用途。

8. 根据权利要求 1 所述的方法，其特征在于：安全认证数据库中的软件安全信息包括软件是否认证为安全，是否病毒程序，是否木马程序，是否存在易受攻击的漏洞。

9. 根据权利要求 1 所述的方法，其特征在于：用于计算的可执行文件包括.exe 文件，.dll 文件，.sys 文件，特定平台上解释执行的脚本文件。

9. 根据权利要求 1 所述的方法，其特征在于：所述的监控程序，其功能包括监控计算机上软件的执行过程，在软件执行之前，计算软件可执行文件的唯一特征码，提交认证服务器进行认证，并根据认证服务器的反馈信息对软件是否继续执行进行判断。

10. 根据权利要求 1 所述的方法，其特征在于：认证服务器和监控程序可以共存于同一台计算机上，也可以分布在不同的计算机上，二者之间可以通过客户/服务器，或者浏览器/服务器的形式进行通信，二者之间可以采用包括 TCP/IP 在内的各种通讯协议进行通信。

一种基于软件身份认证技术的计算机安全保护方法

一．技术领域

本发明涉及计算机应用技术领域，涉及一种计算机安全的保护方法。利用本方法可以建立一种提供计算机安全保护服务的基础设施。利用本方法也可以设计一种提高计算机安全性的应用软件。本方法通过限制未经安全认证的软件在计算机上的执行，提高计算机系统的安全性。

二．背景技术

防止计算机病毒的传播危害，是计算机安全领域的一个重要课题。在《中华人民共和国计算机信息系统安全保护条例》中，计算机病毒的定义是："计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码"。由此可见，计算机病毒可以是一个独立编制的可执行文件，也可以是插入其它计算机程序中的一组可执行指令或程序代码。无论病毒以哪种形式存在，传统的杀毒软件，都是基于一种称为"特征匹配"的工作原理进行病毒检测。其工作原理是首先在杀毒软件里面制作一个关于病毒特征的数据库，在杀毒的时候就根据这些病毒特征对检查对象逐个扫描，如果发现被检查对象存在和已知病毒特征库中的某种特征相匹配的特征段，就定义为发现病毒。传统杀毒软件的原则是：阻止已知有害软件的运行。设计思想是基于对已知非安全软件的发现，只对病毒特征匹配成功的文件加以阻止或者隔离，因此无法实现对未知非安全文件的监控。相对于以病毒为代表的非安全文件出现时间而言，传统杀毒软件的查杀能力是滞后的。只有当这个非安全软件被发现，被报告，并被公认为有破坏性后，才会纳入传统杀毒软件的查杀范围之类。随着病毒技术的改进，以及互联网建设的发展，新病毒的出现频率和传播速度都得到了很大的提高。固有的滞后性，使传统杀毒软件对这些新型的病毒防不胜防，无法彻底避免危害的产生。

另一类方法是基于文件自保护的思想，例如已经公开的发明"微机病毒防治的软件自保护方法"（公开号：CN1068205A）和"计算机软件保护方法"（公开号：CN1155700A）。这种方法都是设法在文件自身添加具有唯一性特征的信息，在程序开始运行的时候，首先检查文件当前的特征信息是否与自身储存的特征信息一致，并由此判断文件是否被非法篡改，进而采取相应的措施。这类方法可以在一定程度上防止软件被病毒程序修改，但也存在着明显的缺陷：1.显然不适用于对病毒为独立可执行文件的情况。换言之，病毒程序自成一体，不修改任何文件，则这类方法无能为力；2.不排除病毒可以在程序被执行前，先行篡改程序，然后根据篡改后的文件状态，使用同样的方法重新计算文件的特征信息，然后替换掉旧有的特征信息。

除了防范病毒攻击，防止黑客直接利用软件的设计漏洞对计算机系统进行攻击，也是当前计算机安全

领域的重要课题。其中最典型的莫过于“缓冲区溢出”漏洞。虽然“缓冲区溢出”攻击是一种非常“古老”的攻击技术（甚至 1988 年 11 月爆发的“莫里斯蠕虫”就利用了“缓冲区溢出”的原理），但它对计算机系统的安全威胁依然很大。杀毒软件和基于文件自保护的方法可以一定程度上防止病毒的入侵，但对利用软件漏洞而进行的直接攻击却无能为力。目前如何防止这类攻击，尚无一个统一，有效的方法和工具，基本上依赖于系统管理员对计算机系统安全性的了解程度和改善计算机系统功能的水平，常见的方法就是及时打上最新的系统补丁。

除此以外，随着互联网技术的发展，各种“木马”软件，广告软件，也给计算机安全带来了威胁，给用户的计算机操作带来了不便。对企业而言，如何限制员工在企业内部网络中运行与工作无关，甚至有潜在安全漏洞的软件，也是一个亟待解决的问题。

三. 发明内容

本发明的目的是提供一种以软件身份识别为基础，采用安全认证数据库和认证服务器对软件进行集中认证的计算机系统安全保护方法，使用这种方法建立一个只允许已知可信的安全软件运行的计算机系统环境。

本发明预先建立安全认证数据库以存储软件的特征信息和安全信息，数据库中存储的每个软件都利用可执行文件的唯一特征码进行标识；并基于该安全认证数据库建立具有安全认证功能的服务器程序。当客户端计算机中的某个软件在被执行时，监控程序会计算出该软件的可执行文件的唯一特征码，并提交给认证服务器。认证服务器根据唯一特征码从安全认证数据库中搜索出该软件的安全信息和特征信息，并把这些信息反馈给监控程序，监控程序根据反馈的结果判断软件是否满足安全的需要，是否可以继续执行。

本发明克服了当前杀毒软件和文件自保护这两类方法的不足，引入新的思路 1.“只允许已知可信的安全软件运行”；2.通过查询集中存储的软件特征信息和安全信息，对正在运行软件的安全性进行评估。

“已知可信的安全软件”是指 1.该软件所包含的所有可执行文件唯一特征码存在于认证服务器数据库中，2.经可信赖的权威机构认证，该软件不是病毒或木马等有害程序，也未被病毒和木马加以修改，3.该软件的安全性级别满足计算机环境对软件安全性的要求，不符合上述任一特征的可执行文件，都视为可疑可执行文件，需要经用户专门确认后才能执行。

本发明既可以有效阻止独立存在的病毒程序文件运行，也可以有效阻止被病毒感染修改的程序文件运行，由于只有“已知可信的安全文件才可以执行”，不仅已知的病毒文件可以被有效阻止，未知的具有破坏性的程序也被切断了执行的路径。本发明还可以在一定程度上降低计算机系统受到因程序漏洞而遭受攻击的风险。通过查询认证服务器上存储的安全信息，系统管理员可以了解本计算机系统中各种软件可能存在的漏洞和安全级别，从而在可行的范围内实施系统的升级维护。

使用本发明可以建立一套计算机系统安全保护基础设施。例如可以建立基于互联网的一个安全管理平台，为互联网用户提供软件信息查询服务，计算机安全保护服务等功能。

使用本发明也可以开发一套用于计算机系统安全保护的软件，为企业提供企业软件运行环境的集中统一保护。企业可以建立自己的安全认证数据库和认证服务器，制订本企业适用的安全策略，规范本企业特定遵守的软件运行条件。例如建立企业网络内允许执行的程序列表，禁止用户在企业网络内执行与工作性质无关的软件等。

四．附图说明

下面通过附图和具体实施方式来进一步阐述本发明的内容：

图 1 是实施本发明所建造的计算机环境的系统结构图；

图 2 是在本发明控制下，计算机软件执行过程的详细流程图；

图 3 是实施本发明后的计算机软件执行过程简图。

五．具体实施方式

通过实施本发明，可以建造一个只有已知可信的软件才能运行的安全环境。为实现这一安全环境所必须建造的基础设施包括如图 1 所示的以下三个部分：

1．安全认证数据库；

2．认证服务器程序；

3．监控程序。

安全认证数据库里存储各种软件的特征信息和安全信息。软件特征信息和安全信息的内容和范围可以根据实际的需要进行调整。一般说来，特征信息包括软件的名称，厂商，版本，软件可执行文件名称，软件的用途等等，而安全信息包括软件是否认证为安全，是否病毒程序，是否木马程序，是否存在易受攻击的漏洞等等。这些信息可以被监控程序用来判定某个即将执行的程序是否病毒，是否已经被恶意篡改，是否存在很容易被攻击的漏洞，从而进一步决定是否允许该程序执行。而系统管理员可以从这些信息中对目前的计算机系统环境安全性进行准确的评估，从而采取合理，可行的措施来对系统进行维护和升级。

在安全认证数据库中如何对每个软件进行标识是一个难题。本发明采用可执行文件的唯一特征码来实现这一需求。软件所对应的可执行文件的唯一特征码，可作为软件的身份特征。所有的软件都由文件组成，文件从根本来说是一组有序的二进制序列。通过对可执行文件的二进制序列进行数字摘要计算，就可以获得相应可执行文件的唯一特征码。可以完成这类数字摘要计算的算法包括 MD4，MD5，SHA 等。如果可

执行文件的二进制序列内容发生任何变化，例如只有一个二进制数字从0变成了1， 经过数字摘要算法计算出来的唯一特征码就会发生变化。由于这种唯一性的存在，可执行文件的唯一特征码就可以作为证实软件身份的充分必要性标志。这里所涉及的可执行文件包括.exe文件，.dll文件，.sys文件，特定平台上解释执行的脚本文件等。

认证服务器程序需要提供的基本功能包括：1.建立和维护安全认证数据库，2.根据监控程序发送来的文件唯一特征码进行查询，反馈软件的特征信息和安全信息。

认证服务器程序可以提供安全认证数据库信息搜集和信息录入，修改的功能。根据实际情况，搜集信息和录入，修改信息的接口可以采用不同的手段，可以自动进行，也可以手动进行。认证服务器程序的功能根据实际的需求具有很强的可扩展性，例如可以增加软件升级建议，软件安全性顾问，软件恢复等功能。

监控程序安装在需要进行安全认证保护的计算机上。监控程序需要提供的基本功能是监控计算机上软件的执行过程，在软件执行之前，计算软件可执行文件的唯一特征码，提交认证服务器进行认证，并根据认证服务器的反馈信息对软件是否继续执行进行判断。系统管理员根据实际情况制订安全策略用于作为判断软件是否可以继续执行的标准，例如病毒程序，木马程序不许运行，未知或未经认证安全的程序在给出提示前提下由用户决定是否执行等。安全策略起着调节监控程序对计算机监控力度的作用。监控程序可以以系统服务，驱动程序或普通进程的方式运行。

认证服务器和监控程序可以共存于同一台计算机上，也可以分布在不同的计算机上，二者之间可以通过客户/服务器，或者浏览器/服务器的形式进行通信。二者之间可以采用包括TCP/IP在内的各种通讯协议进行通信。

监控程序的功能根据实际的需求也具有很强的可扩展性，例如可以帮助系统管理员了解计算机系统环境，了解当前系统安全性等功能。

本发明的实施包括四个环节，分别是：

1. 建立安全认证数据库

2. 建立并运行认证服务器

3. 设计允许软件运行的安全策略

4. 安装并运行监控程序

在实施本发明并受到保护的计算机中，软件执行流程包括如图2所示的如下七个步骤，分别是：

1. 某软件被操作系统调用；

2. 监控程序对该软件的可执行文件进行扫描，生成文件的唯一特征码；

3. 监控程序把文件唯一特征码发送给认证服务器；

4. 认证服务器收到唯一特征码，查询安全认证数据库；

5. 认证服务器把查询到的软件信息，或者把未查到软件的消息反馈给监控程序；

6. 监控程序根据收到的消息，调用安全策略进行比较判断；

7. 监控程序根据判断结果，允许软件运行或者禁止软件运行。

以上所述只是本发明可实现功能的框架描述，更多的变化，更多的功能细节都可用以上内容为核心，添加到本发明中来，从而提供给本发明的用户更实用，更强大的控制能力和服务能力。所以所有与之相关的改动，改进和应用也都包含在本发明的精神和范围内。

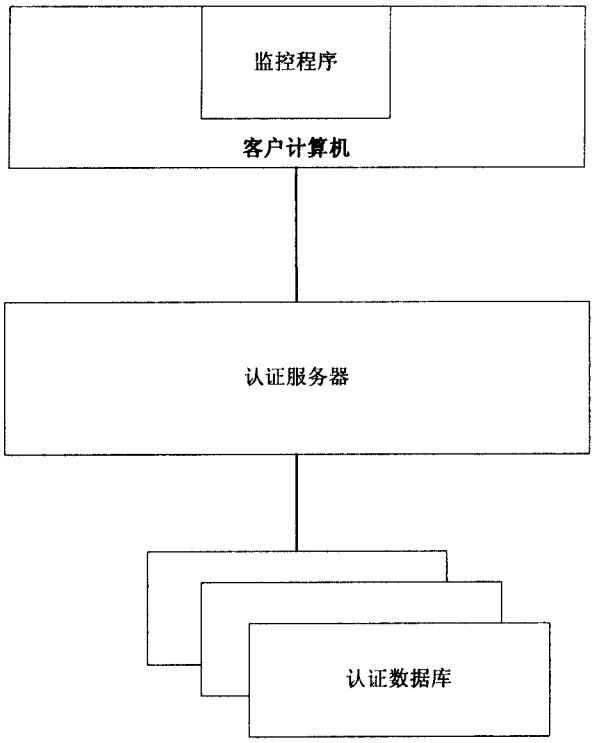


图 1

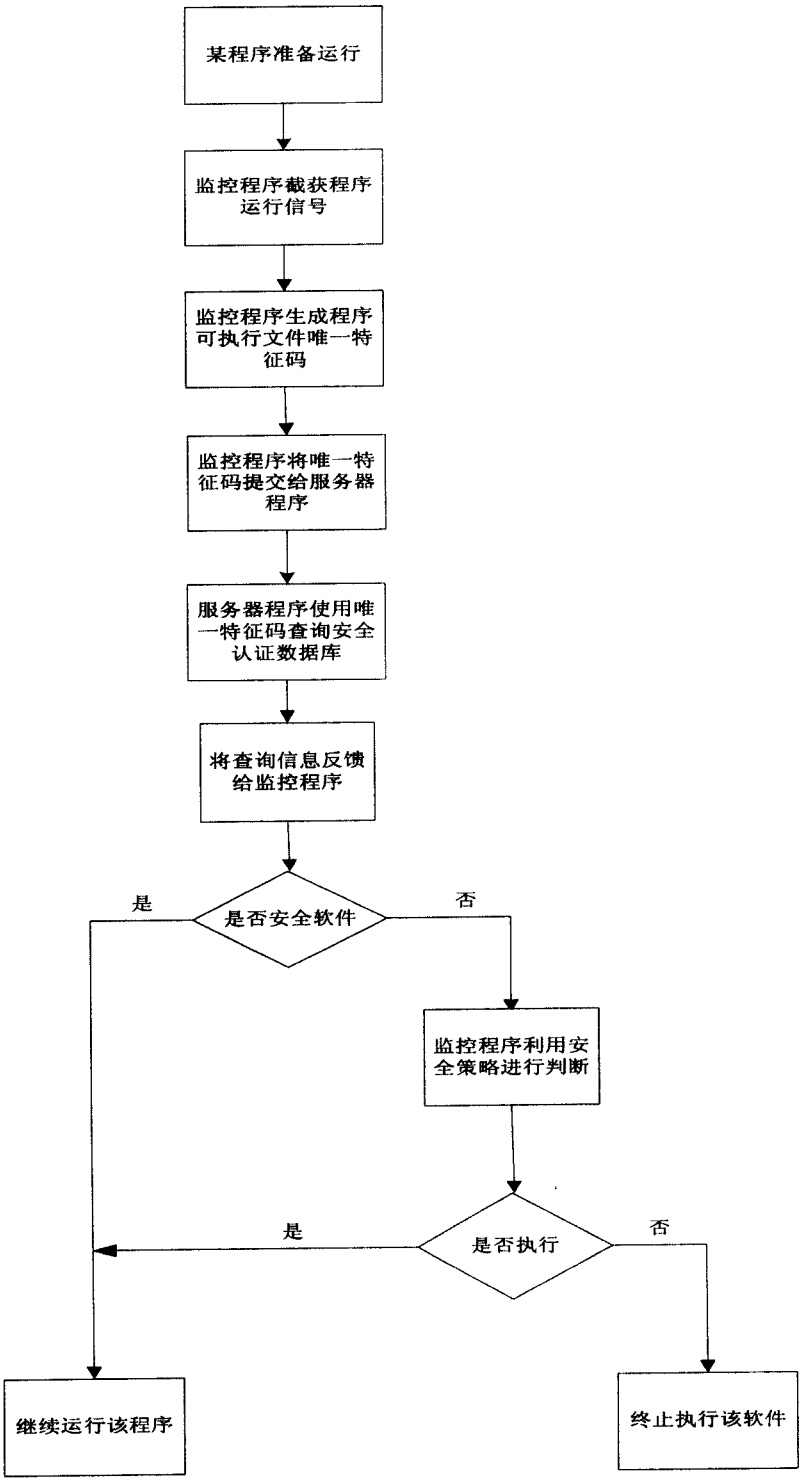

某程序准备运行
监控程序截获程序运行信号
监控程序生成程序可执行文件唯一特征码
监控程序将唯一特征码提交给服务器程序
服务器程序使用唯一特征码查询安全认证数据库
将查询信息反馈给监控程序
是否安全软件
是
否
监控程序利用安全策略进行判断
是否执行
是
否
继续运行该程序
终止执行该软件

图 2

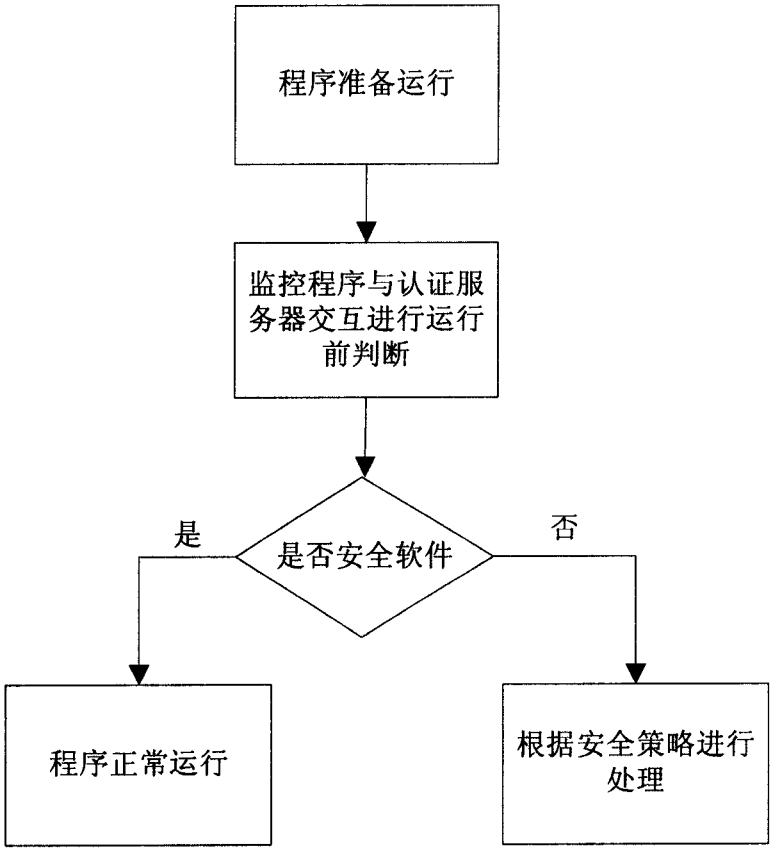


图 3