(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 107423581 B
(45)授权公告日 2019.04.12

(21)申请号 201710641046.5

(22)申请日 2017.07.31

(65)同一申请的已公布的文献号
申请公布号 CN 107423581 A

(43)申请公布日 2017.12.01

(73)专利权人 北京深思数盾科技股份有限公司
地址 100193 北京市海淀区西北旺东路10号院东区5号楼5层510

(72)发明人 孙吉平 张伟双

(74)专利代理机构 北京金信知识产权代理有限公司 11225
代理人 黄威 邓玉婷

(51)Int.Cl.
G06F 21/10(2013.01)

(56)对比文件
CN 102385671 A,2012.03.21,全文.
CN 104123493 A,2014.10.29,全文.
CN 103377319 A,2013.10.30,全文.
CN 101639880 A,2010.02.03,全文.
CN 104424402 A,2015.03.18,全文.
US 2003/0233547 A1,2003.12.18,全文.
US 2007/0174624 A1,2007.07.26,全文.
CN 104133832 A,2014.11.05,说明书第[0057]-[0071],[0150]-[053],[0161]-[0182]段.

审查员 王秋苹

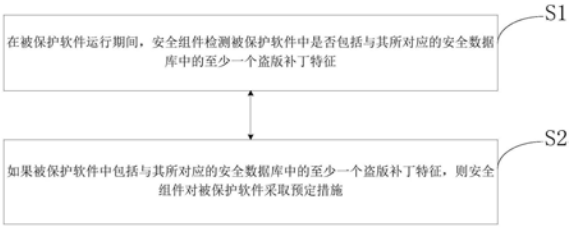
权利要求书3页 说明书8页 附图2页

(54)发明名称

软件的保护方法和装置

(57)摘要

根据本发明的一个方面,提供了一种软件的保护方法和装置,其中,根据本发明的保护方法,预先设置与被保护软件对应的安全数据库,安全数据库中包括:盗版补丁特征;使用安全组件对被保护软件进行保护;根据本发明的方法包括:在被保护软件运行期间,安全组件检测被保护软件中是否包括与其所对应的安全数据库中的至少一个盗版补丁特征;如果被保护软件中包括与其所对应的安全数据库中的至少一个盗版补丁特征,则安全组件对被保护软件采取预定措施,根据本发明的方法提高了针对不同的软件所有权的保护力度并缓解了软件开发商在保护软件所有权方面的压力。



CN 107423581 B

1.一种软件的保护方法,其特征在于,预先设置与被保护软件对应的安全数据库,所述安全数据库中包括:盗版补丁特征;使用安全组件对所述被保护软件进行保护,所述安全组件与所述被保护软件具有绑定关系;根据与不同的所述被保护软件对应的特征类型对所述被保护软件分别进行相应检测类型的检测;

所述方法包括:

在所述被保护软件运行期间,所述安全组件检测所述被保护软件中是否包括与其所对应的安全数据库中的至少一个盗版补丁特征;

如果所述被保护软件中包括与其所对应的安全数据库中的至少一个盗版补丁特征,则所述安全组件对所述被保护软件采取预定措施。

2.根据权利要求1所述的方法,其特征在于,所述盗版补丁特征的数量为多个,多个所述盗版补丁特征划分为至少两个类型;

所述安全组件检测所述被保护软件中是否包括与其所对应的安全数据库中的至少一个盗版补丁特征,包括:

所述安全组件检测所述被保护软件中是否包括与其所对应的安全数据库中的至少两个类型的盗版补丁特征;

如果所述被保护软件中包括与其所对应的安全数据库中的至少两个类型的盗版补丁特征,则所述安全组件对所述被保护软件采取预定措施。

3.根据权利要求1或2所述的方法,其特征在于,所述安全数据库存储在所述被保护软件的目录下,和/或,所述安全数据库存储在所述安全组件的目录下。

4.根据权利要求1或2所述的方法,其特征在于,还预先设置有用于存储破解分析工具特征的数据库;

所述方法包括:

所述安全组件检测各个软件中是否包括所述破解分析工具特征;

如果所述安全组件检测到至少一个软件中包括所述破解分析工具特征,则所述安全组件对所述被保护软件采取预定措施。

5.根据权利要求3所述的方法,其特征在于,还预先设置有用于存储破解分析工具特征的数据库;

所述方法包括:

所述安全组件检测各个软件中是否包括所述破解分析工具特征;

如果所述安全组件检测到至少一个软件中包括所述破解分析工具特征,则所述安全组件对所述被保护软件采取预定措施。

6.根据权利要求4所述的方法,其特征在于,所述破解分析工具特征的数量为多个,多个所述破解分析工具特征划分为至少两个类型;

所述安全组件检测各个软件中是否包括所述破解分析工具特征,包括:

所述安全组件检测各个软件中是否包括至少两个类型的破解分析工具特征;

如果至少一个软件中包括至少两个类型的破解分析工具特征,则所述安全组件对所述被保护软件采取预定措施。

7.根据权利要求5所述的方法,其特征在于,所述破解分析工具特征的数量为多个,多个所述破解分析工具特征划分为至少两个类型;

所述安全组件检测各个软件中是否包括所述破解分析工具特征，包括：

所述安全组件检测各个软件中是否包括至少两个类型的破解分析工具特征；

如果至少一个软件中包括至少两个类型的破解分析工具特征，则所述安全组件对所述被保护软件采取预定措施。

8.根据权利要求1或2所述的方法，其特征在于，所述被保护软件为所述安全组件。

9.根据权利要求3所述的方法，其特征在于，所述被保护软件为所述安全组件。

10.根据权利要求4所述的方法，其特征在于，所述被保护软件为所述安全组件。

11.根据权利要求5所述的方法，其特征在于，所述被保护软件为所述安全组件。

12.根据权利要求6所述的方法，其特征在于，所述被保护软件为所述安全组件。

13.根据权利要求7所述的方法，其特征在于，所述被保护软件为所述安全组件。

14.一种软件的保护装置，其特征在于，包括：

安全组件；

预先设置的与被保护软件对应的安全数据库，所述安全数据库中包括：盗版补丁特征；

所述装置配置为使用安全组件对所述被保护软件进行保护，所述安全组件与所述被保护软件具有绑定关系；

所述安全组件配置为在所述被保护软件运行期间，检测所述被保护软件中是否包括与其所对应的安全数据库中的至少一个盗版补丁特征；

所述安全组件配置为在检测到所述被保护软件中包括与其所对应的安全数据库中的至少一个盗版补丁特征的情况下，对所述被保护软件采取预定措施，

其中，根据与不同的所述被保护软件对应的特征类型对所述被保护软件分别进行相应检测类型的检测。

15.根据权利要求14所述的装置，其特征在于，所述盗版补丁特征的数量为多个，多个所述盗版补丁特征划分为至少两个类型；

所述安全组件配置为检测所述被保护软件中是否包括与其所对应的安全数据库中的至少一个盗版补丁特征，包括：

所述安全组件还配置为检测所述被保护软件中是否包括与其所对应的安全数据库中的至少两个类型的盗版补丁特征；

所述安全组件还配置为在检测到所述被保护软件中包括与其所对应的安全数据库中的至少两个类型的盗版补丁特征的情况下，对所述被保护软件采取预定措施。

16.根据权利要求14或15所述的装置，其特征在于，所述安全数据库存储在所述被保护软件的目录下，和/或，所述安全数据库存储在所述安全组件的目录下。

17.根据权利要求14或15所述的装置，其特征在于，还包括：

预先设置的用于存储破解分析工具特征的数据库；

所述装置包括：

所述安全组件还配置为检测各个软件中是否包括所述破解分析工具特征；

所述安全组件还配置为在检测到至少一个软件中包括所述破解分析工具特征的情况下，对所述被保护软件采取预定措施。

18.根据权利要求16所述的装置，其特征在于，还包括：

预先设置的用于存储破解分析工具特征的数据库；

所述装置包括：

所述安全组件还配置为检测各个软件中是否包括所述破解分析工具特征；

所述安全组件还配置为在检测到至少一个软件中包括所述破解分析工具特征的情况下，对所述被保护软件采取预定措施。

19.根据权利要求17所述的装置，其特征在于，所述破解分析工具特征的数量为多个，多个所述破解分析工具特征包括至少两个类型；

所述安全组件配置为检测各个软件中是否包括所述破解分析工具特征，包括：

所述安全组件进一步配置为检测各个软件中是否包括至少两个类型的破解分析工具特征；

所述安全组件进一步配置为在检测到至少一个软件中包括至少两个类型的破解分析工具特征的情况下，对所述被保护软件采取预定措施。

20.根据权利要求18所述的装置，其特征在于，所述破解分析工具特征的数量为多个，多个所述破解分析工具特征包括至少两个类型；

所述安全组件配置为检测各个软件中是否包括所述破解分析工具特征，包括：

所述安全组件进一步配置为检测各个软件中是否包括至少两个类型的破解分析工具特征；

所述安全组件进一步配置为在检测到至少一个软件中包括至少两个类型的破解分析工具特征的情况下，对所述被保护软件采取预定措施。

21.根据权利要求14或15所述的装置，其特征在于，所述被保护软件为所述安全组件。

22.根据权利要求16所述的装置，其特征在于，所述被保护软件为所述安全组件。

23.根据权利要求17所述的装置，其特征在于，所述被保护软件为所述安全组件。

24.根据权利要求18所述的装置，其特征在于，所述被保护软件为所述安全组件。

25.根据权利要求19所述的装置，其特征在于，所述被保护软件为所述安全组件。

26.根据权利要求20所述的装置，其特征在于，所述被保护软件为所述安全组件。

软件的保护方法和装置

技术领域

[0001] 本发明涉及软件保护，尤其涉及一种软件的保护方法和装置。

背景技术

[0002] 软件开发商发布软件后，经常被盗版问题困扰。盗版(又称「翻版」)指在未经所有权人同意的情况下，对其作品、出版物进行复制、再分发的行为，以及以此行为制成的侵权产品。虽然在很多国家和地区，盗版者的这种行为被定义为侵犯知识产权的违法行为，甚至犯罪行为，会受到所在国的处罚。

[0003] 在软件领域，所谓盗版软件，通常由盗版者对软件进行例如增加附加文件作为盗版补丁等方式的处理从而使消费者可以避开软件所有者相关的验证而使用该软件的功能，通常盗版软件无法提供合法的权利证书(版权证书)、也不能为用户提供售后服务，然而消费者由于盗版软件的价格低廉或免费还是倾向于使用盗版软件。

[0004] 由于现在社会的软件(或软件产品)本身迭代较快，软件开发商如果采取司法手段来解决盗版问题，不但维权成本高，而且时效性差。因而每当遇到盗版，软件开发商常用方法是自己花费大量人力和时间来对市面上所搜集的盗版问题进行分析，定制相应的加密方案，再重新发布软件二进制版本来解决该盗版问题。通过这种方法来处理软件盗版问题的缺点在于：

[0005] 1.增加了软件开发商的开发成本，并且需要有专人来处理相应的工作，因此整体维权成本上升；

[0006] 2.由于上述安全相关的处理方法与软件本身的逻辑没有太大关系，普通的软件开发商通常并不擅长，在处理时力不从心，不能达到保证软件所有权不受侵犯的预期效果；

[0007] 3、每当遇到盗版，需要重新发布软件的版本，处理此问题比较被动。

发明内容

[0008] 为了提高针对不同的软件所有权的保护力度并缓解软件开发商在保护软件所有权方面的压力，本发明提供了一种软件的保护方法和装置。

[0009] 根据本发明的一个方面，提供了一种软件的保护方法，在该保护方法中，预先设置与被保护软件对应的安全数据库，安全数据库中包括：盗版补丁特征；使用安全组件对被保护软件进行保护；

[0010] 根据本发明的方法包括：

[0011] 在被保护软件运行期间，安全组件检测被保护软件中是否包括与其所对应的安全数据库中的至少一个盗版补丁特征；

[0012] 如果被保护软件中包括与其所对应的安全数据库中的至少一个盗版补丁特征，则安全组件对被保护软件采取预定措施。

[0013] 其中，根据本发明的方法，被保护软件中集成有接口及静态库；

[0014] 安全组件通过被保护软件中的接口及静态库与被保护软件具有绑定关系；

[0015] 在被保护软件启动时通过接口及静态库启用安全组件。

[0016] 其中，根据本发明的方法，盗版补丁特征的数量为多个，多个盗版补丁特征划分为至少两个类型；

[0017] 安全组件检测被保护软件中是否包括与其所对应的安全数据库中的至少一个盗版补丁特征，包括：

[0018] 安全组件检测被保护软件中是否包括与其所对应的安全数据库中的至少两个类型的盗版补丁特征；

[0019] 如果被保护软件中包括与其所对应的安全数据库中的至少两个类型的盗版补丁特征，则安全组件对被保护软件采取预定措施。

[0020] 可选地，盗版补丁特征包括以下至少一种类型：

[0021] 内存类型的盗版补丁特征；

[0022] 窗口名称类型的盗版补丁特征；

[0023] 进程类型的盗版补丁特征。

[0024] 优选地，根据本发明的方法，安全数据库存储在被保护软件的目录下，和/或，安全数据库存储在安全组件的目录下。

[0025] 进一步地，根据本发明的方法，还预先设置有用于存储破解分析工具特征的数据库；

[0026] 方法包括：

[0027] 安全组件检测各个软件中是否包括破解分析工具特征；

[0028] 如果安全组件检测到至少一个软件中包括破解分析工具特征，则安全组件对被保护软件采取预定措施。

[0029] 可选地，根据本发明的方法，破解分析工具特征的数量为多个，多个破解分析工具特征划分为至少两个类型；

[0030] 安全组件检测各个软件中是否包括破解分析工具特征，包括：

[0031] 安全组件检测各个软件中是否包括至少两个类型的破解分析工具特征；

[0032] 如果至少一个软件中包括至少两个类型的破解分析工具特征，则安全组件对被保护软件采取预定措施。

[0033] 可选地，根据本发明的方法，破解分析工具特征包括以下至少一种类型：

[0034] 内存类型的破解分析工具特征；

[0035] 窗口名称类型的破解分析工具特征；

[0036] 进程类型的破解分析工具特征；

[0037] 优选地，根据本发明的方法，被保护软件为安全组件。

[0038] 优选地，根据本发明的方法，还包括：

[0039] 安全组件检测被保护软件运行环境中的运行环境信息和各个软件，并且将运行环境信息和各个软件运行过程中产生的数据上传至安全服务端；

[0040] 所述安全组件从安全服务端接收反馈数据，其中，反馈数据包括以下至少一种：新的盗版补丁特征、新的破解分析工具特征和新的安全补丁，反馈数据由安全服务端根据运行环境信息和各个软件运行过程中产生的数据生成。

[0041] 进一步地，根据本发明的方法，还包括：

[0042] 若安全组件接收到的反馈数据中包括新的安全补丁，则被保护软件用安全补丁进行升级；

[0043] 若安全组件接收到的反馈数据中包括新的盗版补丁特征和/或新的破解分析工具特征，则安全组件将新的盗版补丁特征和/或新的破解分析工具特征更新到安全数据库内。

[0044] 此外，安全组件还包括安全组件主体，方法进一步包括：

[0045] 在客户端包括多个安全组件情况下，通过其中版本较高的安全组件的安全组件主体对客户端的所有被保护软件分别根据它们各自的特征类型相应检测类型的检测。

[0046] 根据本发明的另一个方面，提供了一种软件的保护装置，其包括：

[0047] 安全组件；

[0048] 预先设置与被保护软件对应的安全数据库，安全数据库中包括：盗版补丁特征；

[0049] 装置配置为使用安全组件对被保护软件进行保护；

[0050] 安全组件配置为在被保护软件运行期间，检测被保护软件中是否包括与其所对应的安全数据库中的至少一个盗版补丁特征；

[0051] 安全组件配置为在被保护软件中包括与其所对应的安全数据库中的至少一个盗版补丁特征的情况下，对被保护软件采取预定措施。

[0052] 其中，根据本发明的装置，盗版补丁特征的数量为多个，多个盗版补丁特征划分为至少两个类型；

[0053] 安全组件配置为检测被保护软件中是否包括与其所对应的安全数据库中的至少一个盗版补丁特征，包括：

[0054] 安全组件还配置为检测被保护软件中是否包括与其所对应的安全数据库中的至少两个类型的盗版补丁特征；

[0055] 安全组件还配置为在被保护软件中包括与其所对应的安全数据库中的至少两个类型的盗版补丁特征的情况下，对被保护软件采取预定措施。

[0056] 可选地，盗版补丁特征包括以下至少一种类型：

[0057] 内存类型的盗版补丁特征；

[0058] 窗口名称类型的盗版补丁特征；

[0059] 进程类型的盗版补丁特征。

[0060] 可选地，根据本发明的装置，安全数据库存储在被保护软件的目录下，和/或，安全数据库存储在安全组件的目录下。

[0061] 进一步地，根据本发明的装置还包括：

[0062] 预先设置有用于存储破解分析工具特征的数据库；

[0063] 装置包括：

[0064] 安全组件还配置为检测各个软件中是否包括破解分析工具特征；

[0065] 安全组件还配置为在检测到至少一个软件中包括破解分析工具特征的情况下，对被保护软件采取预定措施。

[0066] 优选地，根据本发明的装置，破解分析工具特征的数量为多个，多个破解分析工具特征包括至少两个类型；

[0067] 安全组件配置为检测各个软件中是否包括破解分析工具特征，包括：

[0068] 安全组件进一步配置为检测各个软件中是否包括至少两个类型的破解分析工具

特征；

[0069] 安全组件进一步配置为的至少一个软件中包括至少两个类型的破解分析工具特征的情况下，对被保护软件采取预定措施。

[0070] 可选地，根据本发明的装置，破解分析工具特征包括以下至少一种类型：

[0071] 内存类型的破解分析工具特征；

[0072] 窗口名称类型的破解分析工具特征；

[0073] 进程类型的破解分析工具特征。

[0074] 优选地，根据本发明的装置，被保护软件为安全组件。

[0075] 优选地，根据本发明的装置，安全组件还被配置为检测被保护软件运行环境中的运行环境信息和各个软件，并且将运行环境信息和各个软件运行过程中产生的数据上传至安全服务端；

[0076] 安全组件还被配置为从安全服务端接收反馈数据，其中，反馈数据包括以下至少一种：新的盗版补丁特征、新的破解分析工具特征和新的安全补丁，反馈数据由安全服务端根据运行环境信息和各个软件运行过程中产生的数据生成。

[0077] 本发明的有益效果在于：

[0078] 根据本发明的方法，安全组件根据对应于不同软件的安全数据库中的盗版补丁特征和/或破解分析工具特征，对目标软件进行了不同广度和深度的检测，从而实现对不同软件进行定制处理；通过对运行中的不同盗版软件进行数据统计和分析，深度定位不同的盗版原因；

[0079] 通过针对不同软件的盗版补丁特征和/或破解分析工具特征的类型的不同，对目标软件进行了不同类型的检测，能够做到有的放矢，提高检测的深度和效率；

[0080] 通过下发形式对针对不同盗版软件进行安全补丁的下发，从而达到使不同盗版软件失效的目的；

[0081] 统计当前补丁工作情况，盗版解决情况，并进一步跟踪；

[0082] 而这其中，软件开发商并不需要做太多工作，更不需要了解其工作原理，不用投入专门的人力，只需要专注于自身业务即可。

附图说明

[0083] 图1为根据本发明的软件保护方法的一个实施方式的流程图；

[0084] 图2为根据本发明的软件的保护装置的一个实施方式的框图；

[0085] 图3为根据本发明的软件保护方法的一个优选实施例的示意图。

具体实施方式

[0086] 如图1所示为根据本发明的一个实施例的软件的保护方法，该方法主要使用安全组件对被保护软件进行保护，即，本发明中所谓的被保护软件即为目标软件。其中，安全组件例如可以是反黑引擎。在该保护方法中，预先设置与被保护软件对应的安全数据库，安全数据库中包括：盗版补丁特征；使用安全组件对被保护软件进行保护；

[0087] 根据本发明的方法包括：

[0088] S1，在被保护软件运行期间，安全组件检测被保护软件中是否包括与其所对应的

安全数据库中的至少一个盗版补丁特征；

[0089] S2，如果被保护软件中包括与其所对应的安全数据库中的至少一个盗版补丁特征，则安全组件对被保护软件采取预定措施。该预定措施可以包括使被保护软件无法运行，或者可以运行当前的功能却不可以再进行功能升级因而不能使用将来软件开发商发布的升级功能等等。

[0090] 其中，根据本发明的方法，被保护软件中集成有接口及静态库；安全组件通过被保护软件中的接口及静态库与被保护软件具有绑定关系；在被保护软件启动时通过接口及静态库启用安全组件。被保护软件和安全组件的绑定可以理解为将两者功能绑定，从而在用户使用被保护软件时必须同时运行安全组件，并且也可以理解，被保护软件以安全组件作为与外界通信的“接口”，使得盗版商无法将安全组件从被保护软件分离而不影响被保护软件的功能。

[0091] 其中，根据本发明的方法，盗版补丁特征的数量为多个，多个盗版补丁特征划分为至少两个类型，可选地，盗版补丁特征包括以下至少一种类型：内存类型的盗版补丁特征；窗口名称类型的盗版补丁特征；进程类型的盗版补丁特征；

[0092] 安全组件检测被保护软件中是否包括与其所对应的安全数据库中的至少一个盗版补丁特征，包括：安全组件检测被保护软件中是否包括与其所对应的安全数据库中的至少两个类型的盗版补丁特征；如果被保护软件中包括与其所对应的安全数据库中的至少两个类型的盗版补丁特征，则安全组件对被保护软件采取预定措施。

[0093] 优选地，根据本发明的方法，安全数据库存储在被保护软件的目录下，和/或，安全数据库存储在安全组件的目录下，例如，各个被保护软件分别对应的安全数据库均存储在安全组件的目录下，又例如，各个被保护软件共享同一个安全数据库，该安全数据库存储在安全组件的目录下。

[0094] 进一步地，根据本发明的方法，还预先设置有用于存储破解分析工具特征的数据库；

[0095] 方法包括：

[0096] 安全组件检测各个软件中是否包括破解分析工具特征；

[0097] 如果安全组件检测到至少一个软件中包括破解分析工具特征，则安全组件对被保护软件采取预定措施。

[0098] 可选地，根据本发明的方法，破解分析工具特征的数量为多个，多个破解分析工具特征划分为至少两个类型；安全组件还检测各个软件中是否包括至少两个类型的破解分析工具特征；如果至少一个软件中包括至少两个类型的破解分析工具特征，则安全组件对被保护软件采取预定措施。

[0099] 可选地，根据本发明的方法，破解分析工具特征包括以下至少一种类型：内存类型的破解分析工具特征；窗口名称类型的破解分析工具特征；进程类型的破解分析工具特征。

[0100] 优选地，根据本发明的方法，所述被保护软件除了可以是安全组件之外的软件外，所述被保护软件还可以为安全组件，即安全组件实现自我性能的监控。具体的，当被保护软件是安全组件时，与安全组件对应的数据库中包括盗版补丁特征和破解分析工具特征，其中，盗版补丁特征用于检测安全组件是否是盗版的，破解分析工具特征用于检测运行环境中的恶意软件；对于安全组件之外的其它被保护软件，其数据库中可以只包括与被保护软

件有关的盗版补丁，用以检测被保护软件是否是盗版。

[0101] 优选地，根据本发明的方法，还包括：

[0102] 安全组件检测被保护软件运行环境中的运行环境信息和各个软件，并且将运行环境信息和各个软件运行过程中产生的数据上传至安全服务端；安全服务端根据运行环境信息和各个软件运行过程中产生的数据来获取新的盗版补丁特征和/或新的破解分析工具特征，并可选地生成新的安全补丁，并将这些特征和安全补丁作为反馈数据下发到所有安全组件，由于运行环境信息能够实时/定期上传，因此，安全服务端能够实时/定期掌握被保护软件是否存在被盗版现象，从而根据实时/定期检测到的运行环境信息和各个软件运行过程中产生的数据生成最新的盗版补丁，从而做出应对策略，将盗版情况限定在可控范围内；

[0103] 所述安全组件从安全服务端接收反馈数据，其中，反馈数据包括以下至少一种：新的盗版补丁特征、新的破解分析工具特征和新的安全补丁，反馈数据由安全服务端根据运行环境信息和各个软件运行过程中产生的数据生成。此外，即，盗版补丁特征和/或破解分析工具特征的获取渠道并非单一由安全组件上传，而是还可以包括由安全开发商或者安全服务端的操作人员主动收集，然后通过安全服务端的特定接口传输至安全服务端中，这种方式作为补充的盗版补丁特征和/或破解分析工具特征获取渠道使得本发明的技术方案能获取更为全面的盗版补丁特征和/或破解分析工具特征，从而做出更为全面的应对策略。优选地，可以在获取被保护软件的功能升级补丁的时候来获取反馈数据，从而节约更新次数。

[0104] 进一步地，根据本发明的方法还包括：若安全组件接收到的反馈数据中包括新的安全补丁，则被保护软件用安全补丁进行升级；若安全组件接收到的反馈数据中包括新的盗版补丁特征和/或新的破解分析工具特征，则安全组件将新的盗版补丁特征和/或新的破解分析工具特征更新到安全数据库内，例如可以更新到所有被保护软件的安全数据库中，也可以只更新到与新的盗版补丁特征和/或新的破解分析工具特征具有一定关联关系的被保护软件的安全数据库中。

[0105] 此外，安全组件还包括安全组件主体，方法进一步包括：在客户端包括多个安全组件情况下，通过其中版本较高的安全组件的安全组件主体对客户端的所有被保护软件分别根据它们各自的特征类型进行相应检测类型的检测。即，同一个用户端的不同的被保护软件可以应用同一个安全组件主体根据与不同的被保护软件相对应的安全数据来进行检测。

[0106] 根据本发明的另一个实施例，提供了一种软件的保护装置，其包括：

[0107] 安全组件21；

[0108] 预先设置与被保护软件对应的安全数据库22，安全数据库中包括：盗版补丁特征；

[0109] 根据本发明的装置配置为使用安全组件对被保护软件进行保护；

[0110] 安全组件21配置为在被保护软件运行期间，检测被保护软件中是否包括与其所对应的安全数据库中的至少一个盗版补丁特征；

[0111] 安全组件21配置为在被保护软件中包括与其所对应的安全数据库中的至少一个盗版补丁特征的情况下，对被保护软件采取预定措施。

[0112] 其中，根据本发明的装置，盗版补丁特征的数量为多个，多个盗版补丁特征划分为至少两个类型；

[0113] 安全组件配置为检测被保护软件中是否包括与其所对应的安全数据库中的至少一个盗版补丁特征，包括：

[0114] 安全组件还配置为检测被保护软件中是否包括与其所对应的安全数据库中的至少两个类型的盗版补丁特征；

[0115] 安全组件还配置为在被保护软件中包括与其所对应的安全数据库中的至少两个类型的盗版补丁特征的情况下，对被保护软件采取预定措施。通过两个类型的盗版补丁特征的组合可以更为准确地判断出软件中是否存在盗版补丁。

[0116] 可选地，盗版补丁特征包括以下至少一种类型：

[0117] 内存类型的盗版补丁特征；

[0118] 窗口名称类型的盗版补丁特征；

[0119] 进程类型的盗版补丁特征。

[0120] 可选地，根据本发明的装置，安全数据库存储在被保护软件的目录下，和/或，安全数据库存储在安全组件的目录下。

[0121] 进一步地，根据本发明的装置还包括：

[0122] 预先设置有用于存储破解分析工具特征的数据库；

[0123] 装置包括：

[0124] 安全组件还配置为检测各个软件中是否包括破解分析工具特征；

[0125] 安全组件还配置为在检测到至少一个软件中包括破解分析工具特征的情况下，对被保护软件采取预定措施。

[0126] 根据本发明的一个优选实施方式，在根据本发明的装置中，破解分析工具特征的数量为多个，多个破解分析工具特征包括至少两个类型；

[0127] 安全组件配置为检测各个软件中是否包括破解分析工具特征，包括：

[0128] 安全组件进一步配置为检测各个软件中是否包括至少两个类型的破解分析工具特征；

[0129] 安全组件进一步配置为的至少一个软件中包括至少两个类型的破解分析工具特征的情况下，对被保护软件采取预定措施。由于破解分析工具特征存在特征程度强弱之别(即，情况I，凭一软件中检测到特征程度强的特征，则安全组件可以断定该软件为破解分析工具；情况II，在一软件中检测到特征程度较弱的特征时，安全组件可以确定该软件为破解分析工具，也可以将检测到的特征上传到安全服务端进行进一步的判断)，在本实施例中，即属于情况II，安全组件在一软件中只检测到一个程度较弱的类型的破解分析工具特征的情况下，难以确定该软件是否为破解分析工具，因此，通过破解分析工具特征的组合(两个或多个破解分析工具特征的组合)可以断定该软件为破解分析工具，解决了需要由安全服务端进一步判断的麻烦情况。但是，本实施方式中的两个特征并不限于特征程度弱的特征的组合，也可以与特征程度强的特征进行组合。至于如何区别强弱特征，则可以由安全服务端预先根据不同的软件及相应的特征进行区分。盗版补丁特征与破解分析工具特征在本实施例中的原理相似。

[0130] 可选地，根据本发明的装置，破解分析工具特征包括以下至少一种类型：

[0131] 内存类型的破解分析工具特征；

[0132] 窗口名称类型的破解分析工具特征；

[0133] 进程类型的破解分析工具特征。

[0134] 优选地，根据本发明的装置，被保护软件为安全组件。

[0135] 优选地，根据本发明的装置，安全组件还被配置为检测被保护软件运行环境中的运行环境信息和各个软件，并且将运行环境信息和各个软件运行过程中产生的数据上传至安全服务端；

[0136] 安全组件还被配置为从安全服务端接收反馈数据，其中，反馈数据包括以下至少一种：新的盗版补丁特征、新的破解分析工具特征和新的安全补丁，反馈数据由安全服务端根据运行环境信息和各个软件运行过程中产生的数据生成。

[0137] 可以理解，本发明的技术方案是通过网络或其它无线通信媒介实现的。

[0138] 根据本发明的软件的保护方法的实施方式，如图3所示，针对软件U进行保护的方法流程图，具体描述如下：

[0139] 软件U描述

[0140] ①运行环境要求：不可与调试器od.exe(ollydbg.exe)同时运行(即与破解分析工具特征相关)；

[0141] ②需检测已知盗版补丁x.dll(即与盗版补丁特征相关)。

[0142] (一)提取特征

[0143] 针对ollydbg.exe，提取窗口名称：ollydbg，生成特征①，其为窗口类型特征；提取进程名称：ollydbg.exe，生成生成特征②，其为进程名称特征；提取内存数据：从0×40000开始到0×40010的hash值，生成特征③，其为内存特征。其中，窗口名称、进程名称和内存数据为特征类型，而ollydbg、ollydbg.exe和从0×40000开始到0×40010的hash值为对应的特征内容。

[0144] 针对x.dll(省略了特征内容)，提取模块名生成特征④；提取内存数据生成特征⑤；提取文件签名生成特征⑥。

[0145] 以上特征①至⑥均存储至安全数据库中。

[0146] (二)运行时(网络部分未体现)

[0147] 在被检测软件运行时，engine.dll(安全组件主体)根据安全数据库中的特征类型进行窗口检测、进行名称检测、内存数据检测等，以检测是否有相应的特征内容存在。

[0148] 该安全组件根据不同的软件定义了不同的盗版补丁特征和破解分析工具特征，以此实现对不同软件的安全检测和保护。传统杀毒软件可以对当前流行的病毒木马进行检测和查杀，但由于针对性不足，对特定软件的安全需求不能满足。

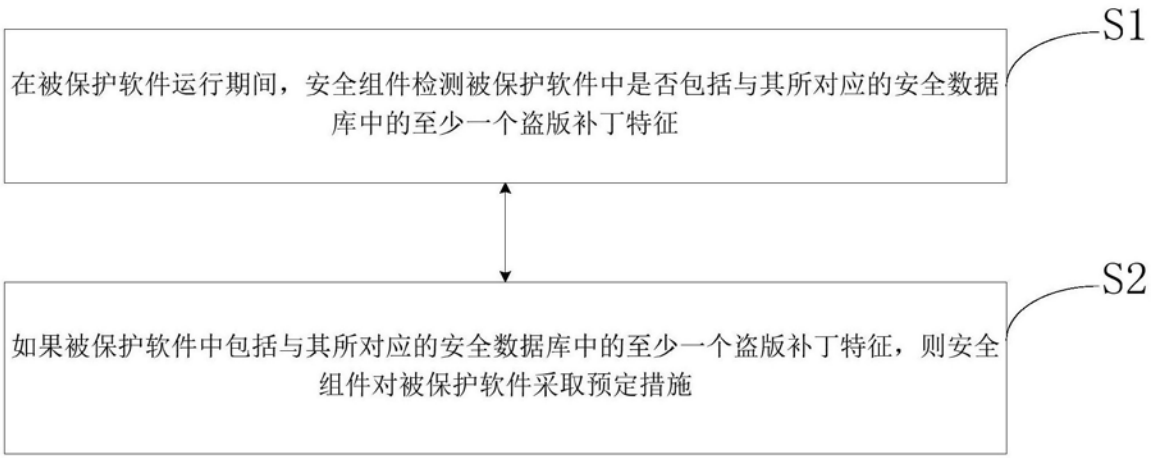

S1
在被保护软件运行期间，安全组件检测被保护软件中是否包括与其所对应的安全数据库中的至少一个盗版补丁特征
S2
如果被保护软件中包括与其所对应的安全数据库中的至少一个盗版补丁特征，则安全组件对被保护软件采取预定措施

图1

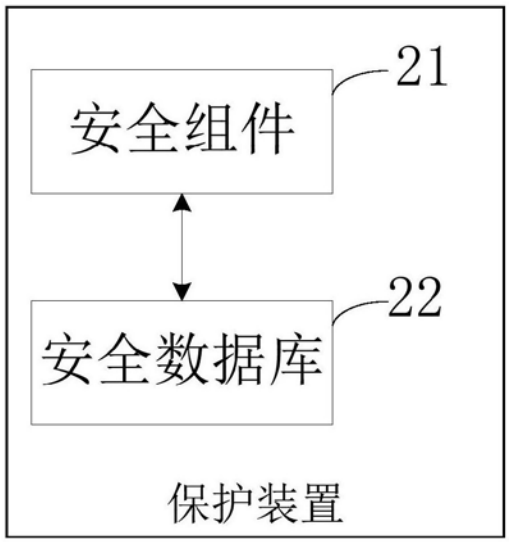

21
安全组件
22
安全数据库
保护装置

图2

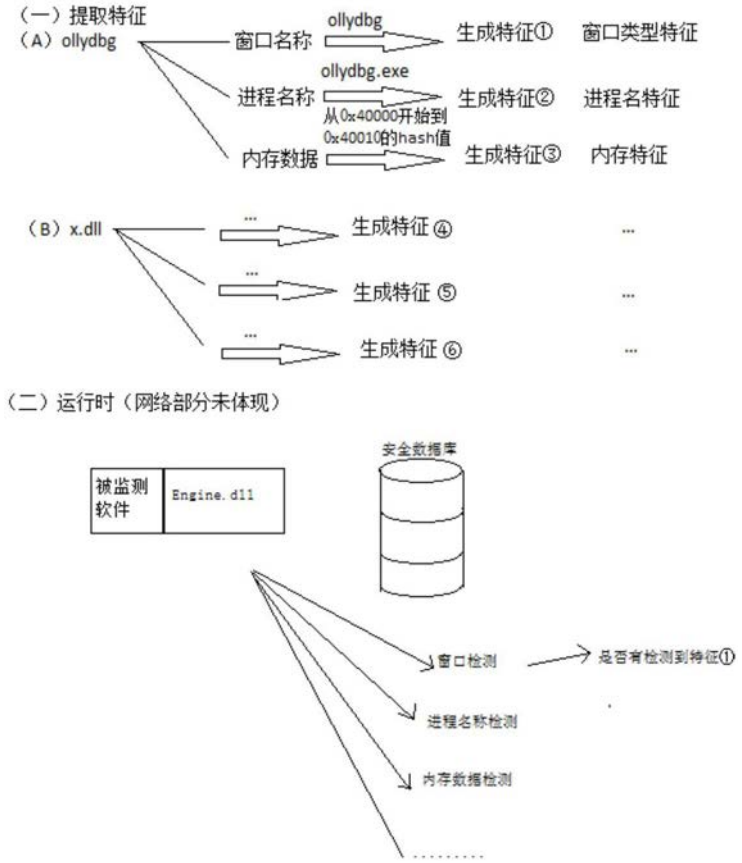

（一）提取特征
（A）ollydbg
窗口名称
ollydbg
生成特征①
窗口类型特征
进程名称
ollydbg.exe
从0x40000开始到
0x40010的hash值
生成特征②
进程名特征
内存数据
生成特征③
内存特征
（B）x.dll
生成特征④
生成特征⑤
生成特征⑥
（二）运行时（网络部分未体现）
被监测
软件
Engine.dll
安全数据库
窗口检测
是否有检测到特征①
进程名称检测
内存数据检测

图3