



(12) 发明专利申请

(10) 申请公布号 CN 102262717 A

(43) 申请公布日 2011.11.30

(21) 申请号 201110201188.2

(22) 申请日 2011.07.18

(71) 申请人 百度在线网络技术(北京)有限公司

地址 100085 北京市海淀区上地十街 10 号
百度大厦

(72) 发明人 田彪

(74) 专利代理机构 北京汉昊知识产权代理事务
所(普通合伙) 11370

代理人 罗朋

(51) Int. Cl.

G06F 21/00 (2006.01)

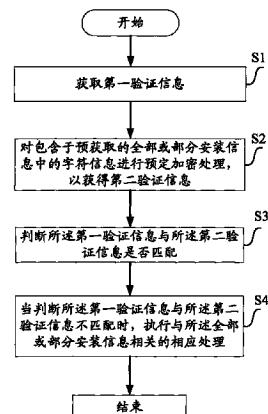
权利要求书 5 页 说明书 22 页 附图 3 页

(54) 发明名称

用于更改原始安装信息及检测安装信息的方
法、装置及设备

(57) 摘要

本发明提供一种用于检测被篡改的安装信息
的方法、装置及设备。根据本发明的方法，先获取
第一验证信息以及对包含于预获取的全部或部分
安装信息中的字符信息进行预定加密处理，以获
得第二验证信息，随后判断所述第一验证信息与
所述第二验证信息是否匹配，当判断所述第一验
证信息与所述第二验证信息不匹配时，执行与所
述全部或部分安装信息相关的相应处理。本发明
的优点包括：可避免因安装信息被篡改而导致计
算机设备遭受病毒等攻击的危险。



1. 一种用于检测被篡改的安装信息的方法,其中,该方法包括以下步骤:

i 获取第一验证信息;

其中,该方法还包括以下步骤:

x 对包含于全部或部分安装信息中的字符信息进行预定加密处理,以获得第二验证信息,其中,所述全部或部分安装信息通过预获取来获得;

其中,该方法还包括以下步骤:

a 判断所述第一验证信息与所述第二验证信息是否匹配;

b 当判断所述第一验证信息与所述第二验证信息不匹配时,执行与所述全部或部分安装信息相关的相应处理。

2. 根据权利要求1所述的方法,其中,所述步骤x还包括以下步骤:

- 根据所述全部或部分安装信息中第一预定位置的字符来获得所述字符信息;

- 对所述字符信息进行所述预定加密处理,以获得所述第二验证信息。

3. 根据权利要求1或2所述的方法,其中,所述步骤i包括以下步骤:

- 获取所述全部或部分安装信息中第二预定位置的待处理信息;

- 对所述待处理信息进行第一预定处理,以获得所述第一验证信息。

4. 根据权利要求1所述的方法,其中,所述步骤i包括以下步骤:

- 根据预获取的部分安装信息来获得所述第一验证信息;

其中,所述步骤x包括以下步骤:

- 对包含于所述部分安装信息中的字符信息进行所述预定加密处理,以获得第二验证信息;

其中,该方法还包括以下步骤:

c 当判断所述第一验证信息与所述第二验证信息匹配时,获取另一部分安装信息,并将所述另一部分安装信息作为所述部分安装信息;

d 重复所述步骤i、步骤x、步骤a和步骤c,直至步骤c中获取另一部分安装信息失败或步骤a中判断所述第一验证信息与所述第二验证信息不匹配。

5. 根据权利要求4所述的方法,其中,所述步骤x包括以下步骤:

- 根据所述部分安装信息中第一预定位置的字符来获得所述字符信息;

- 对所述第一预定位置的字符信息进行所述预定加密处理,以获得所述第二验证信息。

6. 根据权利要求4或5所述的方法,其中,所述步骤i包括以下步骤:

- 由所述部分安装信息中的第二预定位置获取待处理信息;

- 对所述待处理信息进行第一预定处理,以获得所述第一验证信息。

7. 根据权利要求1至6中任一项所述的方法,其中,该方法还包括以下步骤:

- 根据所述安装信息的获取来源,在预定白名单中进行查询;

其中,所述步骤i还包括以下步骤:

- 当未能在所述预定白名单中查询到所述获取来源时,根据已获取的全部或部分安装信息来获得所述第一验证信息;

其中,所述步骤a还包括以下步骤:

- 当未能在所述预定白名单中查询到所述获取来源时,对包含于所述全部或部分安装信息中的字符信息进行所述预定加密处理,以获得所述第二验证信息。

8. 根据权利要求 1 至 7 中任一项所述的方法, 其中, 所述步骤 i 还包括以下步骤 :

- 当获得用户要求基于预获取的全部安装信息来执行安装操作的指令时, 根据所述全部安装信息来获得第一验证信息 ;

其中, 所述步骤 a 还包括以下步骤 :

- 当获得用户要求基于所述全部安装信息来执行安装操作的指令时, 对包含于所述全部安装信息中的字符信息进行所述预定加密处理, 以获得所述第二验证信息。

9. 根据权利要求 1 至 8 中任一项所述的方法, 其中, 所述与全部或部分安装信息相关的相应处理包括以下至少一项 :

- 删除所述全部或部分安装信息 ;

- 当尚未获取全部安装信息时, 停止获取剩余的安装信息 ;

- 将用于提醒该安装信息可能不安全的提示信息呈现给用户 ;

- 将下载所述安装信息的可信网站信息呈现给所述用户。

10. 根据权利要求 9 所述的方法, 其中, 所述与全部或部分安装信息相关的相应处理包括将用于提醒该安装信息可能不安全的提示信息呈现给用户, 其中, 该方法还包括以下步骤 :

- 根据所述用户对所述提示信息反馈的指令信息, 来执行以下操作中的任一项 :

- 删除所述全部或部分安装信息 ;

- 将所述安装信息移动至隔离区 ;

- 根据所述全部或部分安装信息来执行安装操作 ;

- 终止对所述安装信息所执行的操作。

11. 根据权利要求 1 至 10 中任一项所述的方法, 其中, 所述预定加密处理根据预定加密算法来执行。

12. 根据权利要求 11 所述的方法, 其中, 所述预定加密处理还根据预定加密参数来执行。

13. 一种用于在原始安装信息中添加验证信息的方法, 其中, 所述方法还包括以下步骤 :

o. 根据预获取的第一验证信息以及预定字符信息来更改原始安装信息, 以获得未被篡改的安装信息, 其中, 对所述预定字符信息进行预定加密处理能够获取与所述第一验证信息相匹配的第二验证信息。

14. 根据权利要求 13 所述的方法, 其中, 所述步骤 o 中根据所述预定字符信息来更改原始安装信息的步骤包括 :

- 将所述预定字符信息添加至所述原始安装信息的第一预定位置 ; 或者, 将所述预定字符信息在所述原始安装信息中的位置信息作为第一预定位置信息, 添加至所述原始安装信息中。

15. 根据权利要求 13 或 14 所述的方法, 其中, 所述步骤 o 中根据所述第一验证信息来更改原始安装信息的步骤包括 :

- 对所述第一验证信息进行第二预定处理, 以获得待处理信息 ;

- 将所述待处理信息添加至所述原始安装信息的第二预定位置。

16. 一种用于检测被篡改的安装信息的检测装置, 其中, 该检测装置包括 :

第一获取装置,用于获取第一验证信息;

加密装置,用于对包含于全部或部分安装信息中的字符信息进行预定加密处理,以获得第二验证信息,其中,所述全部或部分安装信息通过预获取来获得;

判断装置,用于判断所述第一验证信息与所述第二验证信息是否匹配;

第一执行装置,用于当判断所述第一验证信息与所述第二验证信息不匹配时,执行与所述全部或部分安装信息相关的相应处理。

17. 根据权利要求 16 所述的检测装置,其中,所述加密装置还包括:

第一字符获取装置,用于根据所述全部或部分安装信息中第一预定位置的字符来获得所述字符信息;

第一子加密装置,用于对所述字符信息进行所述预定加密处理,以获得所述第二验证信息。

18. 根据权利要求 16 或 17 所述的检测装置,其中,所述第一获取装置还包括:

第一子获取装置,用于获取所述全部或部分安装信息中第二预定位置的待处理信息;

第一处理装置,用于对所述待处理信息进行第一预定处理,以获得所述第一验证信息。

19. 根据权利要求 16 所述的检测装置,其中,所述第一获取装置包括:

第二子获取装置,用于根据预获取的部分安装信息来获得所述第一验证信息;

其中,所述加密装置包括:

第二子加密装置,用于对包含于所述部分安装信息中的字符信息进行所述预定加密处理,以获得第二验证信息;

其中,该检测装置还包括:

第二获取装置,用于当判断所述第一验证信息与所述第二验证信息匹配时,获取另一部分安装信息,并将所述另一部分安装信息作为所述部分安装信息;

迭代装置,用于触发所述第二子获取装置与第二子加密装置,以使所述第二子获取装置、所述第二子加密装置、所述判断装置及所述第二获取装置重复执行操作,直至所述第二获取装置获取所述另一部分安装信息失败或所述判断装置判断所述第一验证信息与所述第二验证信息不匹配。

20. 根据权利要求 19 所述的检测装置,其中,所述第二子加密装置包括:

第二字符获取装置,用于根据所述部分安装信息中第一预定位置的字符来获得所述字符信息;

第五子加密装置,用于对所述第一预定位置的字符信息进行所述预定加密处理,以获得所述第二验证信息。

21. 根据权利要求 19 或 20 所述的检测装置,其中,所述第二子获取装置包括:

第五子获取装置,用于由所述部分安装信息中的第二预定位置获取待处理信息;

第二处理装置,用于对所述待处理信息进行第一预定处理,以获得所述第一验证信息。

22. 根据权利要求 16 至 21 所述的检测装置,其中,该检测装置还包括:

查询装置,用于根据所述安装信息的获取来源,在预定白名单中进行查询;

其中,所述第一获取装置还包括:

第三子获取装置,用于当未能在所述预定白名单中查询到所述获取来源时,根据已获取的全部或部分安装信息来获得所述第一验证信息;

其中,所述加密装置还包括:

第三子加密装置,用于当未能在所述预定白名单中查询到所述获取来源时,对包含于所述全部或部分安装信息中的字符信息进行所述预定加密处理,以获得所述第二验证信息。

23. 根据权利要求 16 至 22 中任一项所述的检测装置,其中,所述第一获取装置还包括:

第四子获取装置,用于当获得用户要求基于预获取的全部安装信息来执行安装操作的指令时,根据所述全部安装信息来获得第一验证信息;

其中,所述加密装置还包括:

第四子加密装置,用于当获得用户要求基于所述全部安装信息来执行安装操作的指令时,对包含于所述全部安装信息中的字符信息进行所述预定加密处理,以获得所述第二验证信息。

24. 根据权利要求 16 至 23 中任一项所述的检测装置,其中,所述与全部或部分安装信息相关的相应处理包括以下至少一项:

- 删除所述全部或部分安装信息;
- 当尚未获取全部安装信息时,停止获取剩余的安装信息;
- 将用于提醒该安装信息可能不安全的提示信息呈现给用户;
- 将下载所述安装信息的可信网站信息呈现给所述用户。

25. 根据权利要求 24 所述的检测装置,其中,所述与全部或部分安装信息相关的相应处理包括将用于提醒该安装信息可能不安全的提示信息呈现给用户,其中,该检测装置还包括:

第二执行装置,用于根据所述用户对所述提示信息反馈的指令信息,来执行以下操作中的任一项:

- 删除所述全部或部分安装信息;
- 将所述安装信息移动至隔离区;
- 根据所述全部或部分安装信息来执行安装操作;
- 终止对所述安装信息所执行的操作。

26. 根据权利要求 16 至 25 中任一项所述的检测装置,其中,所述预定加密处理根据预定加密算法来执行。

27. 根据权利要求 26 所述的检测装置,其中,所述预定加密处理还根据预定加密参数来执行。

28. 一种用于在原始安装信息中添加验证信息的更改装置,其中,该更改装置用于通过根据预获取的第一验证信息以及预定字符信息来更改原始安装信息,以获得未被篡改的安装信息,其中,对所述预定字符信息进行预定加密处理能够获取与所述第一验证信息相匹配的第二验证信息。

29. 根据权利要求 28 所述的更改装置,其中,所述更改装置包括:

第一子更改装置,用于将所述预定字符信息添加至所述原始安装信息的第一预定位置;或者,将所述预定字符信息在所述原始安装信息中的位置信息作为第一预定位置信息,添加至所述原始安装信息中。

30. 根据权利要求 28 所述的更改装置，其中，所述更改装置包括：

第三处理装置，用于对所述第一验证信息进行第二预定处理，以获得待处理信息；

第二子更改装置，用于将所述待处理信息添加至所述原始安装信息的第二预定位置。

31. 一种第一计算机设备，其中，该计算机设备包括如权利要求 16 至 27 中至少一项所述的检测装置。

32. 一种第二计算机设备，其中，该计算机设备包括如权利要求 28 至 30 中至少一项所述的更改装置。

33. 一种计算机系统，其中，该计算机系统包括如权利要求 31 所述的第一计算机设备以及如权利要求 32 所述的第二计算机设备。

用于更改原始安装信息及检测安装信息的方法、装置及设备

技术领域

[0001] 本发明涉及计算机领域，尤其涉及一种用于检测被篡改的安装信息的方法、装置及设备。

背景技术

[0002] 随着电脑、手机等的普及，越来越多的电脑或手机用户常常会从各种网站下载各类安装信息，例如，QQ 安装包、紫光输入法等，以拓展自身所使用的电脑或手机的应用功能。然而，一旦用户下载的安装信息被添加了病毒，当用户所使用的电脑或手机运行了该安装信息，就会导致系统受到攻击，从而给用户带来难以估量的损失。

[0003] 因此，需要对安装信息进行检测，以确定其是否被篡改，以便确保运行该安装信息的设备的安全。

发明内容

[0004] 本发明的目的是提供一种用于检测被篡改的安装信息的方法、装置及设备。

[0005] 根据本发明的一个方面，提供一种用于检测被篡改的安装信息的方法，其中，该方法包括以下步骤：

[0006] i 获取第一验证信息；

[0007] 其中，该方法还包括以下步骤：

[0008] x 对包含于预获取的全部或部分安装信息中的字符信息进行预定加密处理，以获得第二验证信息，其中，所述全部或部分安装信息通过预获取来获得；

[0009] 其中，该方法还包括以下步骤：

[0010] a 判断所述第一验证信息与所述第二验证信息是否匹配；

[0011] b 当判断所述第一验证信息与所述第二验证信息不匹配时，执行与所述全部或部分安装信息相关的相应处理。

[0012] 根据本发明的另一个方面，还提供了一种用于检测被篡改的安装信息的检测装置，其中，该检测装置包括：

[0013] 第一获取装置，用于获取第一验证信息；

[0014] 加密装置，用于对包含于预获取的全部或部分安装信息中的字符信息进行预定加密处理，以获得第二验证信息，其中，所述全部或部分安装信息通过预获取来获得；

[0015] 判断装置，用于判断所述第一验证信息与所述第二验证信息是否匹配；

[0016] 第一执行装置，用于当判断所述第一验证信息与所述第二验证信息不匹配时，执行与所述全部或部分安装信息相关的相应处理。

[0017] 根据本发明的又一个方面，还提供了一种计算机设备，其中，该计算机设备包括前述的检测装置。

[0018] 与现有技术相比，本发明具有以下优点：1) 由于安装信息中的第一验证信息在诸

如被解析并添加病毒等被篡改过程中,往往由于多种原因,例如,安装信息未被完全解析、因需要添加额外病毒信息等,而导致第一验证信息发生变化,例如,被删除或改变,因此,根据本发明的方法能够通过判断第一验证信息与第二验证信息是否匹配来较为准确地判断安装信息是否被篡改,由此可避免因安装信息被篡改而导致计算机设备遭受病毒等攻击的危险;而且,由于第一验证信息以及第二验证信息均可根据安装信息来获得,使得本发明的方法与硬件或安装信息的获取方式相脱离,适用面较广且实施简便;2) 由于安装信息经过被解析并添加诸如病毒等篡改处理后,由该经过篡改处理的安装信息中获取的预定位置的字符信息往往不同于由未被篡改的安装信息中获取的预定位置的字符信息,由此,对由该经过篡改处理的安装信息中获取的预定位置的字符信息进行预定加密处理后,所获得的第二验证信息与第一验证信息匹配的概率就会大大降低,因此,根据本实施的方法,可进一步提高被篡改安装信息的检出率;3) 可对安装信息进行分段验证,以提前判断安装信息是否可能被篡改。特别是在安装信息的信息量较大的情况下,可以避免花费大量时间下载安装信息后才能验证安装信息是否被篡改的情况;4) 无需再对由可信来源处获得的安装信息进行验证,减少了设备资源消耗;5) 仅在用户要求基于安装信息来进行安装操作时,才启动验证处理,避免了用户因突然收到安装信息可能被篡改的通知而产生突兀感。

附图说明

[0019] 通过阅读参照以下附图所作的对非限制性实施例所作的详细描述,本发明的其它特征、目的和优点将会变得更明显:

- [0020] 图1为本发明一个方面的用于检测被篡改的安装信息的方法的流程图;
- [0021] 图2为图1所示的实施例中步骤S2的一个优选实施例的流程图;
- [0022] 图3为图1所示的实施例中步骤S1的一个优选实施例的流程图;
- [0023] 图4为本发明一个方面的用于检测被篡改的安装信息的检测装置示意图;
- [0024] 图5为图4所示的实施例中加密装置的一个优选实施例的示意图;
- [0025] 图6为图4所示的实施例中第一获取装置的一个优选实施例的示意图;
- [0026] 附图中相同或相似的附图标记代表相同或相似的部件。

具体实施方式

[0027] 下面结合附图对本发明作进一步详细描述。

[0028] 图1示出了本发明一个方面的用于检测被篡改的安装信息的方法的流程图。其中,本发明的在原始安装信息中添加验证信息的方法主要通过更改装置来实现;本发明的检测被篡改的安装信息的方法主要通过检测装置来实现。该检测装置包括但不限于:1) 在执行本发明的步骤前已安装在第一计算机设备中且能够实现本发明方案的诸如应用模块、操作系统、处理控制器等的装置;2) 由本发明中的安装信息所携带并安装至所述第一计算机设备中的装置。本发明中,将检测装置在前述1) 和 2) 中所安装至的第一计算机设备统称为检测装置所属第一计算机设备。该更改装置包括但不限于安装在第二计算机设备中且能够实现本发明方案的诸如应用模块、操作系统、处理控制器等的装置。前述第一以及第二计算机设备为一种能够按照事先存储的程序,自动、高速地进行大量数值计算和各种信息处理的现代化智能电子设备,其硬件包括但不限于微处理器、FPGA、DSP、嵌入式设备等。

[0029] 需要说明的是,所述用户设备及网络设备仅为举例,其他现有的或今后可能出现的用户设备、网络设备或网络如可适用于本发明,也应包含在本发明保护范围以内,并以引用方式包含于此。

[0030] 在图1所示步骤S1之前,包含于第二计算机设备中的更改装置根据预获取的第一验证信息以及预定字符信息来更改原始安装信息,以获得未被篡改的安装信息,其中,对所述预定字符信息进行预定加密处理能够获取与所述第一验证信息相匹配的第二验证信息。

[0031] 其中,所述第二验证信息与未被篡改的安装信息中的第一验证信息匹配的匹配方式包括但不限于:1)所述第二验证信息与所述第一验证信息相同;2)第二验证信息与所述第一验证信息符合预定匹配规则。

[0032] 需要说明的是,上述举例仅为更好地说明本发明的技术方案,而非对本发明的限制,本领域技术人员应该理解,任何第二验证信息与所述第一验证信息匹配的匹配方式,均应包含在本发明的范围内。

[0033] 本领域技术人员应该理解,所述预定字符信息与第一验证信息基于前述匹配方式来确定。

[0034] 当匹配方式为前述1)中所述情形,所述预定字符信息为任何经过预定加密处理能获得第一验证信息的字符信息。例如,若第一验证信息通过基于DES算法对字符串X1进行加密处理来获得,所述预定字符信息即为所述字符串X1,所述预定加密处理即为DES加密算法。

[0035] 当匹配方式为前述2)中所述情形,所述预定字符信息与第一验证信息基于预定匹配规则来确定。

[0036] 例如,预定匹配规则为:第一验证信息包含完整的第二验证信息。若所述预定字符信息为字符串X2,对字符串X2进行预定加密处理获得所述第二验证信息Y1,相应地,所述第一验证信息通过在所述第二验证信息Y1头部和尾部增加无意义信息来获得。

[0037] 又例如,预定匹配规则为:所述第一验证信息为所述第二验证信息的反逻辑。若所述预定字符信息为01,对所述预定字符信息为01进行预定加密处理获得所述第二验证信息1100,相应地,所述第一验证信息为0011=1100。

[0038] 需要说明的是,上述举例仅为更好地说明本发明的技术方案,而非对本发明的限制,本领域技术人员应该理解,预定匹配规则并非以所示为限。

[0039] 所述更改装置获取第一验证信息及预定字符信息的方式包括但不限于:1)获取人工输入的第一验证信息及预定字符信息;2)由存储设备中获取第一验证信息及预定字符信息等;3)先获取人工输入的或存储设备中已存储的预定字符信息,再对预定字符信息进行第四预定处理来获得第一验证信息,其中,该第四预定处理包括任何能够生成与第二验证信息相匹配的第一验证信息的处理方式;4)先获取人工输入的或存储设备中已存储的第一验证信息,再对第一验证信息进行第三预定处理来获得预定字符信息,其中,该第三预定处理包括任何能够生成符合前述内容中所限定的预定字符信息的处理方式。

[0040] 其中,所述更改装置根据获取的第一验证信息来更改原始安装信息的方式包括但不限于以下任一项:

[0041] 1)将第一验证信息加入所述原始安装信息中。例如,所述更改装置生成包含预获取的第一验证信息且文件名为预定文件名“aaa.txt”的文件,并将该文件添加至原始安装

信息；再例如，所述更改装置将所述第一验证信息直接加入所述原始安装信息的预定文件名为 abc.html 的文件中。

[0042] 优选地，所述更改装置在所述原始安装信息中添加能够将已添加至原始安装信息中的第一验证信息复制至其他计算机设备中的预定存储位置的可执行文件，以使获取了添加第一验证信息的其他计算机设备能由该安装信息以外的位置获取第一验证信息。

[0043] 2) 所述更改装置先对所述第一验证信息进行第二预定处理，以获得待处理信息；随后再将所述待处理信息添加至所述原始安装信息的第二预定位置。其中，所述第二预定处理包括任何能对信息进行处理的处理方式，优选地，第二预定处理的处理方式包括：分解、加密、解密等等。所述第二预定位置包括但不限于：一个或多个预定文件、各个预定文件中或其文件名中的一个或多个预定位置、预定路径和 / 或预定排序位的文件、预定路径和 / 或预定排序位的文件中或其文件名中的一个或多个预定位置等。例如，所述更改装置基于预定字符串长度来将第一验证信息“abcdef”划分为分别包含 3 个字符的两个子验证信息“abc”与“def”，并将该两个子验证信息“abc”与“def”分别添加至原始安装信息中文件名为 a2.ini 的文件中第 2 行和文件名为 a3.log 的文件中第 8 至 10 个字符。又例如，所述更改装置基于第一验证信息“1110”为“0101”与“1011”的异或值来将该第一验证信息“1110”分解为“0101”与“1011”两个子验证信息，并将该“0101”与“1011”两个子验证信息分别添加至原始安装信息中按照文件大小排序在第五位的文件的最后一行和倒数第八行。

[0044] 需要说明的是，上述举例仅为更好地说明本发明的技术方案，而非对本发明的限制，本领域技术人员应该理解，任何根据预获取的第一验证信息来更改原始安装信息的实现方式，均应包含在本发明的范围内。

[0045] 其中，所述更改装置根据预获取的预定字符信息来更改原始安装信息的方式包括但不限于以下一项：

[0046] 1) 将预定字符信息添加至用于加入原始安装信息中的检测装置中，以便当其他获取了该已添加检测装置的安装信息的计算机设备运行该检测信息时，检测装置能直接基于该预定字符信息来生成第二验证信息。例如，所述更改装置将预定字符信息“a\$&”加入检测装置中，并将检测装置加入原始安装信息中，则当其他设备获取了更改后的安装信息并运行其中的检测装置时，检测装置能直接基于该预定字符信息“a\$&”来生成第二验证信息。

[0047] 2) 将预定字符信息添加至原始安装信息的第一预定位置；或者，将预定字符信息在原始安装信息中的位置信息作为第一预定位置信息添加至原始安装信息中。其中，所述第一预定位置包括但不限于：一个或多个预定文件、各个预定文件中或其文件名中的一个或多个预定位置、预定路径和 / 或预定排序位的文件、预定路径和 / 或预定排序位的文件中或其文件名中的一个或多个预定位置等。例如，所述更改装置确定所获取的预定字符信息与原始安装信息中文件名为 a2.d11 的文件中第 3 至 7 个字符相同，则所述更改装置将第一预定位置信息“a2.d11 文件中第 3 至 7 个字符”加入原始安装信息中。又例如，第一预定位置为文件名为 a3.doc 文件中第 4 行，则所述更改装置将所获取的预定字符信息加入原始安装信息中文件名为 a3.doc 的文件第四行。

[0048] 需要说明的是，上述举例仅为更好地说明本发明的技术方案，而非对本发明的限制，本领域技术人员应该理解，任何根据预获取的预定字符信息来更改原始安装信息的实现方式，均应包含在本发明的范围内。

[0049] 第一计算机设备可通过诸如由网络中下载、由其所能够访问的存储设备中获取等多种方式来获得全部或部分安装信息，并能够通过下述步骤 S1 至 S4 来检测所获得的全部或部分安装信息是否被篡改。

[0050] 在步骤 S1 中，所述检测装置获取第一验证信息。

[0051] 其中，所述第一验证信息预先置于未被篡改的安装信息中。其中，所述安装信息包括能够自动或者根据用户指令来进行安装操作的安装相关信息，例如，QQ 安装包，又例如，输入法安装信息等。

[0052] 所述检测装置获取第一验证信息的方式由前述更改装置根据预获取的第一验证信息来更改原始安装信息的方式来确定，具体地，检测装置获取第一验证信息的方式包括但不限于以下实现方式：

[0053] 1) 本实现方式中，前述更改装置将第一验证信息加入所述原始安装信息中。检测装置由预获取的全部或部分安装信息中直接获取第一验证信息。

[0054] 例如，当所述检测装置所属的第一计算机设备已获取全部安装信息，并触发所述检测装置，则所述检测装置由所述全部安装信息中获取预定文件名为“aaa. txt”的文件，并将该“aaa. txt”文件中的全部内容作为第一验证信息；又例如，当所述第一计算机设备已获取部分安装信息，并触发所述检测装置，则所述检测装置由所述部分安装信息中获取预定文件名为 abc. html 的文件中预定位置的信息，并将该预定位置的信息作为第一验证信息。

[0055] 2) 本实现方式中，前述更改装置将待处理信息加入所述原始安装信息的第二预定位置，检测装置由所述全部或部分安装信息中的第二预定位置获取待处理信息，并对所获取的待处理信息进行第一预定处理来获得第一验证信息。该方式将在后续图 3 所示的实施例中进行详述。

[0056] 3) 本实现方式中，前述更改装置在所述原始安装信息中添加将第一验证信息复制至计算机设备中的预定存储位置的可执行文件，检测装置由预获取的全部或部分安装信息以外的预定存储位置处获取第一验证信息。例如，当安装信息全部下载至检测装置所属第一计算机设备中时，第一计算机设备即根据安装信息的属性来运行该安装信息中的用于复制第一验证信息的可执行文件，来将安装信息中的第一验证信息复制至第一计算机设备中的预定存储位置；则当用户发出要求基于该安装信息来执行安装操作的指令时，检测装置由该预定存储位置处获得第一验证信息。

[0057] 需要说明的是，上述举例仅为更好地说明本发明的技术方案，而非对本发明的限制，本领域技术人员应该理解，根据预获取的全部或部分安装信息来获得第一验证信息的实现方式，均应包含在本发明的范围内。

[0058] 接着，在步骤 S2 中，所述检测装置对包含于预获取的全部或部分安装信息中的字符信息进行预定加密处理，以获得第二验证信息。

[0059] 其中，所述字符信息为前述更改装置用于更改原始安装信息的预定字符信息；所述检测装置对包含于所述全部或部分安装信息中的字符信息进行预定加密处理所获得的第二验证信息，与前述更改装置根据第一验证信息以及预定字符信息来更改原始安装信息后所获得的未被篡改的全部或部分安装信息中的第一验证信息相匹配。

[0060] 其中，所述检测装置基于预定加密算法来对字符信息进行前述预定加密处理；优

选地,检测装置还基于预定加密参数,例如,加密后的信息的字符数量等,来对字符信息进行前述预定加密处理。更优选地,所述预定加密算法包括但不限于:DES 算法、3DES 算法、IDEA 算法、DSA 算法、MD5 算法等。

[0061] 其中,检测装置基于字符信息来获得第二验证信息的方式包括但不限于:

[0062] 1) 本实现方式中,前述更改装置将预定字符信息加入原始安装信息中的检测装置中,检测装置直接基于所加入的预定字符信息来生成第二验证信息。例如,检测装置包含于安装信息中,并当安装信息已全部下载至所述检测装置所属的第一计算机设备后,检测装置安装至第一计算机设备中。则检测装置直接采用预定 IDEA 加密算法,对其包含的预定字符信息“a\$&”进行加密处理,来获得第二验证信息。

[0063] 2) 本实现方式中,前述更改装置将预定字符信息添加至原始安装信息的第一预定位置;或者,将预定字符信息在原始安装信息中的位置信息作为第一预定位置信息添加至原始安装信息中。检测装置先根据第一预定位置的字符来获得字符信息,再对所获得的字符信息进行预定加密处理来获得第二验证信息。其中,该获取字符信息的方式以及对字符信息进行预定加密处理来获得第二验证信息的方式将在后续图 2 所示的实施例中予以详述。

[0064] 需要进一步说明的是,步骤 S1 和步骤 S2 并无先后顺序。

[0065] 在步骤 S3 中,所述检测装置判断所述第一验证信息与所述第二验证信息是否匹配。

[0066] 其中,所述检测装置判断所述第二验证信息与所述第一验证信息是否匹配的实现方式包括但不限于:

[0067] 1) 本实现方式中,前述未被篡改的安装信息中的第一验证信息和对未被篡改的安装信息中的预定字符信息进行预定加密处理后所获得的第二验证信息相同。检测装置通过判断步骤 S2 中获得的第二验证信息与步骤 S1 中获得的第一验证信息是否相同来判断步骤 S2 中获得的第二验证信息与步骤 S1 中获得的第一验证信息是否匹配。

[0068] 2) 本实现方式中,未被篡改的安装信息中的第一验证信息和对未被篡改的安装信息中的预定字符信息经过进行预定加密处理后所获得的第二验证信息符合预定匹配规则。检测装置通过判断步骤 S2 中获得的第二验证信息与步骤 S1 中获得的第一验证信息是否符合预定匹配规则,来判断步骤 S2 中获得的第二验证信息与步骤 S1 中获得的第一验证信息是否匹配。

[0069] 例如,预定匹配规则为:第一验证信息包含完整的第二验证信息。检测装置通过判断步骤 S1 中获得的第一验证信息是否包含完整的步骤 S2 中获得的第二验证信息,判断步骤 S2 中获得的第二验证信息与步骤 S1 中获得的第一验证信息是否匹配。

[0070] 又例如,预定匹配规则包括:前述未被篡改的安装信息中的第一验证信息为第二验证信息的反逻辑;检测装置在步骤 S1 中获得第一验证信息“0011”,在步骤 S2 中获得第二验证信息“1100”,则检测装置基于 $1100 = \overline{0011}$,判断步骤 S2 中获得的第二验证信息与步骤 S1 中获得的第一验证信息匹配。

[0071] 又例如,预定匹配规则包括:前述未被篡改的安装信息中的第一验证信息以及对未被篡改的安装信息中的预定字符信息进行预定加密处理后所获得的第二验证信息中的一者包含另一者;检测装置在步骤 S1 中获得第一验证信息“abd123”,在步骤 S2 中获

得第二验证信息“ccc”，则所述检测装置基于“abd123”不包含“ccc”，并且“ccc”不包含“abd123”，判断步骤 S2 中获得的第二验证信息与步骤 S1 中获得的第一验证信息不匹配。

[0072] 需要说明的是，上述举例仅为更好地说明本发明的技术方案，而非对本发明的限制，本领域技术人员应该理解，判断所述第二验证信息与所述第一验证信息是否匹配的判断方式，均应包含在本发明的范围内。

[0073] 此外，需要说明的是，本领域技术人员应该理解，当所述检测装置判断所述第一验证信息与所述第二验证信息不匹配时，则表明所述检测装置获得的第一验证信息所来自的全部或部分安装信息已被篡改。

[0074] 接着，在步骤 S4 中，当判断所述第一验证信息与所述第二验证信息不匹配时，所述检测装置执行与所述全部或部分安装信息相关的相应处理。

[0075] 其中，所述检测装置执行的相应处理包括但不限于以下至少一项：

[0076] 1) 删除所述全部或部分安装信息；

[0077] 2) 当尚未获取全部安装信息时，停止获取剩余的安装信息；

[0078] 3) 将用于提醒该安装信息可能不安全的提示信息呈现给用户；

[0079] 4) 将下载所述安装信息的可信网站信息呈现给所述用户。

[0080] 例如，当尚未获取全部安装信息时，检测装置停止获取剩余的安装信息的操作，并将用于提醒该安装信息可能不安全的提示信息呈现给用户等。

[0081] 优选地，当所述与全部或部分安装信息相关的相应处理包括将用于提醒该安装信息可能不安全的提示信息呈现给用户时，根据本发明的方法还包括根据所述用户对所述提示信息反馈的指令信息，来执行以下操作中的任一项的步骤：

[0082] 1) 删除所述全部或部分安装信息；

[0083] 2) 将所述安装信息移动至隔离区；

[0084] 3) 根据所述全部或部分安装信息来执行安装操作；

[0085] 4) 终止对所述安装信息所执行的操作。例如，所述检测装置停止安装操作但不删除安装信息等。

[0086] 例如，当用户基于提示信息反馈删除指令时，检测装置删除所述全部或部分安装信息。

[0087] 需要说明的是，上述举例仅为更好地说明本发明的技术方案，而非对本发明的限制，本领域技术人员应该理解，当判断所述第一验证信息与所述第二验证信息不匹配时，任何执行与所述全部或部分安装信息相关的相应处理的实现方式，均应包含在本发明的范围内。

[0088] 由于安装信息中的第一验证信息在诸如被解析并添加病毒等被篡改过程中，往往由于多种原因，例如，安装信息未被完全解析、因需要添加额外病毒信息等，而导致第一验证信息发生变化，例如，被删除或改变，因此，根据本发明的方法能够通过判断第一验证信息与第二验证信息是否匹配来较为准确地判断安装信息是否被篡改，由此可避免因安装信息被篡改而导致计算机设备遭受病毒等攻击的危险；而且，由于第一验证信息以及第二验证信息均可根据安装信息来获得，使得本发明的方法与硬件或安装信息的获取方式相脱离，适用面较广且实施简便。

[0089] 图 2 示出了图 1 所示的实施例中步骤 S2 的一个优选实施例的流程图。本实施例

中的步骤 S2 包括步骤 S21 与 S22。

[0090] 在步骤 S21 中,所述检测装置根据所述全部或部分安装信息中第一预定位置的字符来获得字符信息。其中,所述第一预定位置为未被篡改的安装信息中预定字符信息所在的位置。优选地,第一预定位置包括但不限于:一个或多个预定文件、各个预定文件中或其文件名中的一个或多个预定位置、预定路径和 / 或预定排序位的文件、预定路径和 / 或预定排序位的文件中或其文件名中的一个或多个预定位置等。例如,预定文件 abc.txt 包含的全部内容信息,或者,包含的内容信息中第 12 至 15 个字符;又例如,预定文件夹 txb 下按文件名字符降序排序后第二位的文件中包含的全部信息;又例如,对安装信息中所有文件的文件大小进行升序排序后第十位的文件名中的全部信息等。

[0091] 具体地,检测装置直接根据其包含的用于限定字符获取位置的信息,或者,根据更改装置所加入的预定字符信息的第一预定位置信息,确定第一预定位置;并且,检测装置直接将所述全部或部分安装信息中一个第一预定位置的字符作为完整的字符信息;或者,检测装置由所述全部或部分安装信息中的多个第一预定位置分别获得多个字符,并将所获得的多个字符进行诸如组合、变换等处理,来获得字符信息。

[0092] 例如,检测装置直接根据其包含的用于限定字符获取位置的信息,确定第一预定位置包括:1) 文件 wieng.txt 的第 2 至 4 个文件名字符;以及 2) 文件 xoing.doc 包含的内容中第 12 个字符以及第 45 个字符;接着,检测装置访问文件 wieng.txt 以及 xoing.doc,获得文件 wieng.txt 的第 2 至 4 个文件名字符为“ien”,并获得文件 xoing.doc 包含的内容中第 12 和 45 个字符分别为“e”和“t”;接着,检测装置将由 wieng.txt 文件名中获得的字符顺序颠倒,并与文件 xoing.doc 中获得的字符组合,获得字符信息“neiet”。

[0093] 又例如,更改装置将第一预定位置信息加入预定文件 location.txt 中,检测装置访问预定文件 location.txt,获得更改装置加入的第一预定位置信息包括“文件路径: shig\pst\amaz.txt; 字符位置: 文件中第 15-21 个字符”,则检测装置根据文件路径访问文件 amaz.txt,并将其中第 15-21 个字符作为完整的字符信息。

[0094] 需要说明的是,上述举例仅为更好地说明本发明的技术方案,而非对本发明的限制,本领域技术人员应该理解,任何获取所述全部或部分安装信息中第一预定位置的字符信息的实现方式,均应包含在本发明的范围内。

[0095] 接着,在步骤 S22 中,所述检测装置对字符信息进行预定加密处理,以获得所述第二验证信息。

[0096] 其中,所述检测装置对字符信息进行预定加密处理来获得第二验证信息的方式,与图 1 所示实施例的步骤 S2 中检测装置对包含于全部或部分安装信息中的字符信息进行预定加密处理,以获得第二验证信息的方式相同或相似,并以引用的方式包含于此,不再赘述。

[0097] 由于安装信息经过被解析并添加诸如病毒等篡改处理后,由该经过篡改处理的安装信息中获取的第一预定位置的字符信息往往不同于由未被篡改的安装信息中获取的预定位置的字符信息,由此,对由该经过篡改处理的安装信息中获取的第一预定位置的字符信息进行预定加密处理后,所获得的第二验证信息与第一验证信息匹配的概率就会大大降低,因此,根据本实施的方法,可进一步提高被篡改安装信息的检出率。

[0098] 图 3 示出了图 1 所示的实施例中步骤 S1 的一个优选实施例的流程图。其中,本实

施例的步骤 S1 包括步骤 S11 与 S12。

[0099] 在步骤 S11 中,所述检测装置由所述全部或部分安装信息的第二预定位置获取待处理信息。

[0100] 其中,所述第二预定位置为未被篡改的安装信息中的待处理信息所在的位置。优选地,第二预定位置包括但不限于:一个或多个预定文件、各个预定文件中或其文件名中的一个或多个预定位置、预定路径和 / 或预定排序位的文件、预定路径和 / 或预定排序位的文件中或其文件名中的一个或多个预定位置等。

[0101] 具体地,所述检测装置由所述全部或部分安装信息中的一个第二预定位置处获得全部待处理信息;或者,所述检测装置由所述全部或部分安装信息中的多个第二预定位置处分别获得多个待处理信息。

[0102] 其中,所述检测装置由所述全部或部分安装信息的第二预定位置获取待处理信息的方式,与图 1 所示的实施例的步骤 S1 中由预获取的全部或部分安装信息中直接获取第一验证信息的方式相同或相似,并以引用的方式包含于此,不再赘述。

[0103] 接着,在步骤 S12 中,所述检测装置对所述待处理信息进行第一预定处理,以获得所述第一验证信息。

[0104] 其中,所述检测装置对所述待处理信息进行第一预定处理的处理方式,与前述更改装置对第一验证信息进行第二预定处理的处理方式相匹配。例如,所述第二预定处理为拆分,则第一预定处理为合并;又例如,所述第二预定处理为加密,则第一预定处理为解密等等。优选地,第一预定处理的处理方式包括但不限于:合并、加密、解密、值的逻辑运算等等。

[0105] 例如,所述检测装置在步骤 S11 中获取的两个待处理信息分别包括“0101”与“1011”,第一预定处理为求取两个待处理信息的异或值,则所述检测装置求取“0101”与“1011”的异或值“1110”,以作为第一验证信息。

[0106] 又例如,第一预定处理为 MD5 加密处理,则所述检测装置采用预定 MD5 算法,对步骤 S11 中获取的待处理信息进行加密处理,获得第一验证信息。

[0107] 再例如,第一预定处理为按序对多个待处理信息进行合并,则所述检测装置将步骤 S11 中获得的三个待处理信息按照预定顺序进行合并,以将合并后的信息作为第一验证信息等。

[0108] 需要说明的是,上述举例仅为更好地说明本发明的技术方案,而非对本发明的限制,本领域技术人员应该理解,对所述待处理信息进行第一预定处理,以获得所述第一验证信息的处理方式,由前述更改装置对待处理信息进行第二预定处理的处理方式来确定。

[0109] 作为一种优选方式,前述图 1、图 2 及图 3 所示的实施例中的步骤 S1 还包括步骤 S1’(未予图示)、步骤 S2 还包括步骤 S2’(未予图示),根据本发明的方法还包括步骤 S5(未予图示)及 S6(未予图示)。

[0110] 在步骤 S1’ 中,所述检测装置根据预获取的部分安装信息来获得所述第一验证信息。其中,所述检测装置根据预获取的部分安装信息来获得所述第一验证信息的方式,与图 1 所示实施例的步骤 S1 中检测装置获取第一验证信息的方式相同或相似,在此不再赘述。

[0111] 优选地,步骤 S1’ 包括由所述部分安装信息中的第二预定位置获取待处理信息的步骤以及对所述待处理信息进行第一预定处理,以获得所述第一验证信息的步骤。其中,所

述检测装置由所述部分安装信息中的第二预定位置获取待处理信息，并对所述待处理信息进行第一预定处理，以获得所述第一验证信息的方式，与图 3 所示的实施例中检测装置由第二预定位置获取待处理信息，并对所述待处理信息进行第一预定处理，以获得所述第一验证信息的方式相同或相似，在此不再赘述。

[0112] 在步骤 S2' 中，所述检测装置对包含于所述部分安装信息中的字符信息进行预定加密处理，以获得第二验证信息。其中，所述检测装置对包含于所述部分安装信息中的字符信息进行预定加密处理来获得第二验证信息的方式，与在图 1 所示的实施例的步骤 S2 中获得第二验证信息的方式相同或相似，并以引用的方式包含于此，不再赘述。

[0113] 优选地，步骤 S2' 包括获取所述部分安装信息中第一预定位置的字符信息的步骤以及对所述第一预定位置的字符信息进行预定加密处理，以获得所述第二验证信息的步骤。其中，所述检测装置获取所述部分安装信息中第一预定位置的字符信息，并对所述第一预定位置的字符信息进行所述预定加密处理，以获得所述第二验证信息的方式，与图 2 所示的实施例步骤 S2 中获取第一预定位置的字符信息，并对所述第一预定位置的字符信息进行所述预定加密处理，以获得所述第二验证信息的方式相同或相似，并以引用的方式包含于此，不再赘述。

[0114] 接着，检测装置执行图 1、图 2 或图 3 实施例中所述步骤 S3，以判断第一验证信息与第二验证信息是否匹配。

[0115] 在步骤 S5 中，当判断所述第一验证信息与所述第二验证信息匹配时，所述检测装置获取另一部分安装信息，并将所述另一部分安装信息作为所述部分安装信息。

[0116] 其中，所述检测装置获取另一部分安装信息的方式包括但不限于：1) 所述检测装置触发自身所属第一计算机设备执行获取另一部分安装信息的操作；其中，所述第一计算机设备获取另一部分安装信息的获取方式与图 1 所示的实施例的步骤 S1 中所述第一计算机设备预获取部分安装信息的获取方式相同或相似，并以引用的方式包含于此，不再赘述；2) 由已存储所述另一部分安装信息的装置或设备提供给所述检测装置等。

[0117] 需要说明的是，上述举例仅为更好地说明本发明的技术方案，而非对本发明的限制，本领域技术人员应该理解，任何获取另一部分安装信息的实现方式，均应包含在本发明的范围内。

[0118] 接着，在步骤 S6 中，所述检测装置重复所述步骤 S1'、步骤 S2'、步骤 S3 和步骤 S5 的操作，直至在步骤 S5 中获取另一部分安装信息失败或在步骤 S3 中判断所述第一验证信息与所述第二验证信息不匹配。

[0119] 其中，所述检测装置在步骤 S6 中获取另一部分安装信息失败的情形包括但不限于：因已经获取全部安装信息而导致再次获取另一部分安装信息的操作失败、因无法再次访问提供所述另一部分安装信息的网站导致获取所述另一部分安装信息的操作失败、因提供所述另一部分安装信息的设备或装置发生故障导致获取所述另一部分安装信息的操作失败等等。

[0120] 需要说明的是，当所述检测装置获取另一部分安装信息失败后，所述检测装置可以将用于提醒安装信息下载未完成的提示信息呈现给用户，也可以在预定时间后继续获取所述另一部分安装信息的操作等；当所述检测装置在步骤 S3 中判断所述第一验证信息与所述第二验证信息不匹配，则所述检测装置执行前述步骤 S4 的操作。

[0121] 根据本实施例的方法,可对安装信息进行分段验证,以提前判断安装信息是否可能被篡改。特别是在安装信息的信息量较大的情况下,可以避免花费大量时间下载安装信息后才能验证安装信息是否被篡改的情况。

[0122] 作为一种优选方式,本发明的方法还包括步骤 S7(未予图示),前述图 1、图 2 及图 3 所示的实施例中的步骤 S1 还包括步骤 S1”(未予图示)、步骤 S2 还包括步骤 S2”(未予图示)。

[0123] 在步骤 S7 中,所述检测装置根据所述安装信息的获取来源来在预定白名单中进行查询。

[0124] 其中,所述获取来源包括提供所述安装信息的装置、设备或网站的信息等。所述检测装置获取所述获取来源的方式包括但不限于:1) 将由所述安装信息中获取的所述安装信息的来源信息作为所述获取来源;2) 当所述检测装置所属第一计算机设备正在获取所述安装信息时,所述检测装置将所述第一计算机设备所获得的提供所述安装信息的网页的地址信息或设备的标识信息作为所述安装信息的获取来源等。

[0125] 需要说明的是,上述举例仅为更好地说明本发明的技术方案,而非对本发明的限制,本领域技术人员应该理解,任何获取所述安装信息的获取来源的方式的实现方式,均应包含在本发明的范围内。

[0126] 在步骤 S1”中,当未能在所述预定白名单中查询到所述获取来源时,所述检测装置根据已获取的全部或部分安装信息来获得所述第一验证信息。其中,根据已获取的全部或部分安装信息来获得所述第一验证信息已在图 1 所示的实施例的步骤 S1 及图 3 所示的实施例中予以详述,并以引用的方式包含于此,不再赘述。

[0127] 在步骤 S2”中,当未能在所述预定白名单中查询到所述获取来源时,所述检测装置对包含于所述全部或部分安装信息中的字符信息进行所述预定加密处理,以获得所述第二验证信息。其中,对包含于所述全部或部分安装信息中的字符信息进行所述预定加密处理,以获得所述第二验证信息已在图 1 所示的实施例的步骤 S2 及图 2 所示的实施例中予以详述,并以引用的方式包含于此,不再赘述。

[0128] 需要说明的是,步骤 S1”与 S2”并无先后顺序。

[0129] 接着,所述检测装置执行图 1、图 2 或图 3 所示实施例中所述步骤 S3,并当在步骤 S3 中判断第一验证信息与第二验证信息不匹配时,执行步骤 S4。

[0130] 根据本实施例的方法,无需再对由可信来源处获得的安装信息进行验证,减少了设备资源消耗。

[0131] 作为一种优选方式,前述图 1、图 2 及图 3 所示的实施例中的步骤 S1 还包括步骤 S1””(未予图示),步骤 S2 还包括步骤 S2””(未予图示)。

[0132] 在步骤 S1””中,当所述检测装置获得用户要求基于预获取的全部安装信息来执行安装操作的指令时,根据所述全部安装信息来获得第一验证信息。其中,根据预获取的全部安装信息来获得第一验证信息已在图 1 所示的实施例的步骤 S1 及图 3 所示的实施例中予以详述,并以引用的方式包含于此,不再赘述。其中,所述检测装置获得用户要求基于所述全部安装信息来执行安装操作的指令的方式包括但不限于:所述检测装置通过接收诸如键盘、鼠标或触摸笔等人机交互设备发出的信息来获得用户要求基于所述全部安装信息来执行安装操作的指令等。

[0133] 在步骤 S2”中,当所述检测装置获得用户要求基于所述全部安装信息来执行安装操作的指令时,所述检测装置对包含于所述全部安装信息中的字符信息进行所述预定加密处理,以获得所述第二验证信息。其中,对包含于所述全部或部分安装信息中的字符信息进行所述预定加密处理,以获得所述第二验证信息已在图 1 所示的实施例的步骤 S2 及图 2 所示的实施例中予以详述,并以引用的方式包含于此,不再赘述。

[0134] 需要说明的是,步骤 S1”与 S2”并无先后顺序。

[0135] 根据本实施例的方法,仅在用户要求基于安装信息来进行安装操作时,才启动验证处理,避免了用户因突然收到安装信息可能被篡改的通知而产生突兀感。

[0136] 图 4 示出了本发明一个方面的用于检测被篡改的安装信息的检测装置示意图。其中,所述检测装置包括第一获取装置 1、加密装置 2、判断装置 3 及第一执行装置 4。

[0137] 在第一获取装置 1 执行操作之前,包含于第二计算机设备中的更改装置根据预获取的第一验证信息以及预定字符信息来更改原始安装信息,以获得未被篡改的安装信息,其中,对所述预定字符信息进行预定加密处理能够获取与所述第一验证信息相匹配的第二验证信息。

[0138] 其中,所述第二验证信息与未被篡改的安装信息中的第一验证信息匹配的匹配方式包括但不限于:1) 所述第二验证信息与所述第一验证信息相同;2) 第二验证信息与所述第一验证信息符合预定匹配规则。

[0139] 需要说明的是,上述举例仅为更好地说明本发明的技术方案,而非对本发明的限制,本领域技术人员应该理解,任何第二验证信息与所述第一验证信息匹配的匹配方式,均应包含在本发明的范围内。

[0140] 本领域技术人员应该理解,所述预定字符信息与第一验证信息基于前述匹配方式来确定。

[0141] 当匹配方式为前述 1) 中所述情形,所述预定字符信息为任何经过预定加密处理能获得第一验证信息的字符信息。例如,若第一验证信息通过基于 DES 算法对字符串 X1 进行加密处理来获得,所述预定字符信息即为所述字符串 X1,所述预定加密处理即为 DES 加密算法。

[0142] 当匹配方式为前述 2) 中所述情形,所述预定字符信息与第一验证信息基于预定匹配规则来确定。

[0143] 例如,预定匹配规则为:第一验证信息包含完整的第二验证信息。若所述预定字符信息为字符串 X2,对字符串 X2 进行预定加密处理获得所述第二验证信息 Y1,相应地,所述第一验证信息通过在所述第二验证信息 Y1 头部和尾部增加无意义信息来获得。

[0144] 又例如,预定匹配规则为:所述第一验证信息为所述第二验证信息的反逻辑。若所述预定字符信息为 01,对所述预定字符信息为 01 进行预定加密处理获得所述第二验证信息 1100,相应地,所述第一验证信息为 $0011 = \overline{1100}$ 。

[0145] 需要说明的是,上述举例仅为更好地说明本发明的技术方案,而非对本发明的限制,本领域技术人员应该理解,预定匹配规则并非以所示为限。

[0146] 所述更改装置获取第一验证信息及预定字符信息的方式包括但不限于:1) 获取人工输入的第一验证信息及预定字符信息;2) 由存储设备中获取第一验证信息及预定字符信息等;3) 先获取人工输入的或存储设备中已存储的预定字符信息,再对预定字符信息

进行第四预定处理来获得第一验证信息，其中，该第四预定处理包括任何能够生成与第二验证信息相匹配的第一验证信息的处理方式；4) 先获取人工输入的或存储设备中已存储的第一验证信息，再对第一验证信息进行第三预定处理来获得预定字符信息，其中，该第三预定处理包括任何能够生成符合前述内容中所限定的预定字符信息的处理方式。

[0147] 其中，所述更改装置根据获取的第一验证信息来更改原始安装信息的方式包括但不限于以下任一项：

[0148] 1) 将第一验证信息加入所述原始安装信息中。例如，所述更改装置生成包含预获取的第一验证信息且文件名为预定文件名“aaa.txt”的文件，并将该文件添加至原始安装信息；再例如，所述更改装置将所述第一验证信息直接加入所述原始安装信息的预定文件名为abc.html的文件中。

[0149] 优选地，所述更改装置在所述原始安装信息中添加能够将已添加至原始安装信息中的第一验证信息复制至其他计算机设备中的预定存储位置的可执行文件，以使获取了添加第一验证信息的其他计算机设备能由该安装信息以外的位置获取第一验证信息。

[0150] 2) 所述更改装置包括第三处理装置（图未示）以及第二子更改装置（图未示）；第三处理装置对所述第一验证信息进行第二预定处理，以获得待处理信息；随后，第二子更改装置将所述待处理信息添加至所述原始安装信息的第二预定位置。其中，所述第二预定处理包括任何能对信息进行处理的处理方式，优选地，第二预定处理的处理方式包括：分解、加密、解密等等。所述第二预定位置包括但不限于：一个或多个预定文件、各个预定文件中或其文件名中的一个或多个预定位置、预定路径和/或预定排序位的文件、预定路径和/或预定排序位的文件中或其文件名中的一个或多个预定位置等。例如，第三处理装置基于预定字符串长度来将第一验证信息“abcdef”划分为分别包含3个字符的两个子验证信息“abc”与“def”，第二子更改装置将该两个子验证信息“abc”与“def”分别添加至原始安装信息中文件名为a2.ini的文件中第2行和文件名为a3.log的文件中第8至10个字符。又例如，第三处理装置基于第一验证信息“1110”为“0101”与“1011”的异或值来将该第一验证信息“1110”分解为“0101”与“1011”两个子验证信息，第二子更改装置将该“0101”与“1011”两个子验证信息分别添加至原始安装信息中按照文件大小排序在第五位的文件的最后一行和倒数第八行。

[0151] 需要说明的是，上述举例仅为更好地说明本发明的技术方案，而非对本发明的限制，本领域技术人员应该理解，任何根据预获取的第一验证信息来更改原始安装信息的实现方式，均应包含在本发明的范围内。

[0152] 其中，所述更改装置根据预获取的预定字符信息来更改原始安装信息的方式包括但不限于以下一项：

[0153] 1) 将预定字符信息添加至用于加入原始安装信息中的检测装置中，以便当其他获取了该已添加检测装置的安装信息的计算机设备运行该检测信息时，检测装置能直接基于该预定字符信息来生成第二验证信息。例如，所述更改装置将预定字符信息“a\$&”加入检测装置中，并将检测装置加入原始安装信息中，则当其他设备获取了更改后的安装信息并运行其中的检测装置时，检测装置能直接基于该预定字符信息“a\$&”来生成第二验证信息。

[0154] 2) 更改装置包括第一子更改装置（图未示），该第一子更改装置将预定字符信息添加至原始安装信息的第一预定位置；或者，将预定字符信息在原始安装信息中的位置信

息作为第一预定位置信息添加至原始安装信息中。其中，所述第一预定位置包括但不限于：一个或多个预定文件、各个预定文件中或其文件名中的一个或多个预定位置、预定路径和 / 或预定排序位的文件、预定路径和 / 或预定排序位的文件中或其文件名中的一个或多个预定位置等。例如，第一子更改装置确定所获取的预定字符信息与原始安装信息中文件名为 a2.d11 的文件中第 3 至 7 个字符相同，则第一子更改装置将第一预定位置信息“a2.d11 文件中第 3 至 7 个字符”加入原始安装信息中。又例如，第一预定位置为文件名为 a3.doc 文件中第 4 行，则第一子更改装置将所获取的预定字符信息加入原始安装信息中文件名为 a3.doc 的文件第四行。

[0155] 需要说明的是，上述举例仅为更好地说明本发明的技术方案，而非对本发明的限制，本领域技术人员应该理解，任何根据预获取的预定字符信息来更改原始安装信息的实现方式，均应包含在本发明的范围内。

[0156] 第一计算机设备可通过诸如由网络中下载、由其所能够访问的存储设备中获取等多种方式来获得全部或部分安装信息，并能够通过下述第一获取装置 1、加密装置 2、判断装置 3 以及第一执行装置 4 来检测所获得的全部或部分安装信息是否被篡改。

[0157] 第一获取装置 1 获取第一验证信息。

[0158] 其中，所述第一验证信息预先置于未被篡改的安装信息中。其中，所述安装信息包括能够自动或者根据用户指令来进行安装操作的安装相关信息，例如，QQ 安装包，又例如，输入法安装信息等。

[0159] 第一获取装置 1 获取第一验证信息的方式由前述更改装置根据预获取的第一验证信息来更改原始安装信息的方式来确定，具体地，第一获取装置 1 获取第一验证信息的方式包括但不限于以下实现方式：

[0160] 1) 本实现方式中，前述更改装置将第一验证信息加入所述原始安装信息中。第一获取装置 1 由预获取的全部或部分安装信息中直接获取第一验证信息。

[0161] 例如，当所述检测装置所属的第一计算机设备已获取全部安装信息，并触发所述检测装置中的第一获取装置 1，则第一获取装置 1 由所述全部安装信息中获取预定文件名为“aaa.txt”的文件，并将该“aaa.txt”文件中的全部内容作为第一验证信息；又例如，当所述第一计算机设备已获取部分安装信息，并触发第一获取装置 1，则第一获取装置 1 由所述部分安装信息中获取预定文件名为 abc.html 的文件中预定位置的信息，并将该预定位置的信息作为第一验证信息。

[0162] 2) 本实现方式中，前述更改装置将待处理信息加入所述原始安装信息的第二预定位置，第一获取装置 1 由所述全部或部分安装信息中的第二预定位置获取待处理信息，并对所获取的待处理信息进行第一预定处理来获得第一验证信息。该方式将在后续图 6 所示的实施例中进行详述。

[0163] 3) 本实现方式中，前述更改装置在所述原始安装信息中添加将第一验证信息复制至计算机设备中的预定存储位置的可执行文件，第一获取装置 1 由预获取的全部或部分安装信息以外的预定存储位置处获取第一验证信息。例如，当安装信息全部下载至检测装置所属第一计算机设备中时，第一计算机设备即根据安装信息的属性来运行该安装信息中的用于复制第一验证信息的可执行文件，来将安装信息中的第一验证信息复制至第一计算机设备中的预定存储位置；则当用户发出要求基于该安装信息来执行安装操作的指令时，第

一获取装置 1 由该预定存储位置处获得第一验证信息。

[0164] 需要说明的是,上述举例仅为更好地说明本发明的技术方案,而非对本发明的限制,本领域技术人员应该理解,根据预获取的全部或部分安装信息来获得第一验证信息的实现方式,均应包含在本发明的范围内。

[0165] 接着,加密装置 2 对包含于预获取的全部或部分安装信息中的字符信息进行预定加密处理,以获得第二验证信息。

[0166] 其中,所述字符信息为前述更改装置用于更改原始安装信息的预定字符信息;加密装置 2 对包含于所述全部或部分安装信息中的字符信息进行预定加密处理所获得的第二验证信息,与前述更改装置根据第一验证信息以及预定字符信息来更改原始安装信息后所获得的未被篡改的全部或部分安装信息中的第一验证信息相匹配。

[0167] 其中,加密装置 2 基于预定加密算法来对字符信息进行前述预定加密处理;优选地,加密装置 2 还基于预定加密参数,例如,加密后的信息的字符数量等,来对字符信息进行前述预定加密处理。更优选地,所述预定加密算法包括但不限于:DES 算法、3DES 算法、IDEA 算法、DSA 算法、MD5 算法等。

[0168] 其中,加密装置 2 基于字符信息来获得第二验证信息的方式包括但不限于:

[0169] 1) 本实现方式中,前述更改装置将预定字符信息加入原始安装信息中的检测装置中,加密装置 2 直接基于所加入的预定字符信息来生成第二验证信息。例如,检测装置包含于安装信息中,并当安装信息已全部下载至所述检测装置所属的第一计算机设备后,检测装置安装至第一计算机设备中。则加密装置 2 直接采用预定 IDEA 加密算法,对检测装置包含的预定字符信息“a\$&”进行加密处理,来获得第二验证信息。

[0170] 2) 本实现方式中,前述更改装置将预定字符信息添加至原始安装信息的第一预定位置;或者,将预定字符信息在原始安装信息中的位置信息作为第一预定位置信息添加至原始安装信息中。加密装置 2 先根据第一预定位置的字符来获得字符信息,再对所获得的字符信息进行预定加密处理来获得第二验证信息。其中,该获取字符信息的方式以及对字符信息进行预定加密处理来获得第二验证信息的方式将在后续图 5 所示的实施例中予以详述。

[0171] 需要进一步说明的是,第一获取装置 1 和加密装置 2 所执行的操作并无先后顺序。

[0172] 判断装置 3 判断所述第一验证信息与所述第二验证信息是否匹配。

[0173] 其中,判断装置 3 判断所述第二验证信息与所述第一验证信息是否匹配的实现方式包括但不限于:

[0174] 1) 本实现方式中,前述未被篡改的安装信息中的第一验证信息和对未被篡改的安装信息中的预定字符信息进行预定加密处理后所获得的第二验证信息相同。判断装置 3 通过判断加密装置 2 获得的第二验证信息与第一获取装置 1 获得的第一验证信息是否相同来判断加密装置 2 获得的第二验证信息与第一获取装置 1 获得的第一验证信息是否匹配。

[0175] 2) 本实现方式中,未被篡改的安装信息中的第一验证信息和对未被篡改的安装信息中的预定字符信息经过进行预定加密处理后所获得的第二验证信息符合预定匹配规则。判断装置 3 通过判断加密装置 2 获得的第二验证信息与第一获取装置 1 获得的第一验证信息是否符合预定匹配规则,来判断加密装置 2 获得的第二验证信息与第一获取装置 1 获得的第一验证信息是否匹配。

[0176] 例如,预定匹配规则为:第一验证信息包含完整的第二验证信息。检测装置通过判断第一获取装置1获得的第一验证信息是否包含完整的加密装置2获得的第二验证信息,判断加密装置2获得的第二验证信息与第一获取装置1获得的第一验证信息是否匹配。

[0177] 又例如,预定匹配规则包括:前述未被篡改的安装信息中的第一验证信息为第二验证信息的反逻辑;第一获取装置1获得第一验证信息“0011”,加密装置2获得第二验证信息“1100”,则判断装置3基于 $1100 = \overline{0011}$,判断加密装置2获得的第二验证信息与第一获取装置1获得的第一验证信息匹配。

[0178] 又例如,预定匹配规则包括:前述未被篡改的安装信息中的第一验证信息以及对未被篡改的安装信息中的预定字符信息进行预定加密处理后所获得的第二验证信息中的一者包含另一者;第一获取装置1获得第一验证信息“abd123”,加密装置2获得第二验证信息“ccc”,则判断装置3基于“abd123”不包含“ccc”,并且“ccc”不包含“abd123”,判断加密装置2获得的第二验证信息与第一获取装置1获得的第一验证信息不匹配。

[0179] 需要说明的是,上述举例仅为更好地说明本发明的技术方案,而非对本发明的限制,本领域技术人员应该理解,判断所述第二验证信息与所述第一验证信息是否匹配的判断方式,均应包含在本发明的范围内。

[0180] 此外,需要说明的是,本领域技术人员应该理解,当所述检测装置判断所述第一验证信息与所述第二验证信息不匹配时,则表明所述检测装置获得的第一验证信息所来自的全部或部分安装信息已被篡改。

[0181] 接着,当判断所述第一验证信息与所述第二验证信息不匹配时,第一执行装置4执行与所述全部或部分安装信息相关的相应处理。

[0182] 其中,第一执行装置4执行的相应处理包括但不限于以下至少一项:

[0183] 1) 删除所述全部或部分安装信息;

[0184] 2) 当尚未获取全部安装信息时,停止获取剩余的安装信息;

[0185] 3) 将用于提醒该安装信息可能不安全的提示信息呈现给用户;

[0186] 4) 将下载所述安装信息的可信网站信息呈现给所述用户。

[0187] 例如,当尚未获取全部安装信息时,第一执行装置4停止获取剩余的安装信息的操作,并将用于提醒该安装信息可能不安全的提示信息呈现给用户等。

[0188] 优选地,检测装置还包括第二执行装置(图未示);当所述与全部或部分安装信息相关的相应处理包括将用于提醒该安装信息可能不安全的提示信息呈现给用户时,第二执行装置根据所述用户对所述提示信息反馈的指令信息,来执行以下操作中的任一项操作:

[0189] 1) 删除所述全部或部分安装信息;

[0190] 2) 将所述安装信息移动至隔离区;

[0191] 3) 根据所述全部或部分安装信息来执行安装操作;

[0192] 4) 终止对所述安装信息所执行的操作。例如,所述检测装置停止安装操作但不删除安装信息等。

[0193] 例如,当用户基于提示信息反馈删除指令时,第二执行装置删除所述全部或部分安装信息。

[0194] 需要说明的是,上述举例仅为更好地说明本发明的技术方案,而非对本发明的限制,本领域技术人员应该理解,当判断所述第一验证信息与所述第二验证信息不匹配时,任

何执行与所述全部或部分安装信息相关的相应处理的实现方式,均应包含在本发明的范围内。

[0195] 由于安装信息中的第一验证信息在诸如被解析并添加病毒等被篡改过程中,往往由于多种原因,例如,安装信息未被完全解析、因需要添加额外病毒信息等,而导致第一验证信息发生变化,例如,被删除或改变,因此,根据本发明的方法能够通过判断第一验证信息与第二验证信息是否匹配来较为准确地判断安装信息是否被篡改,由此可避免因安装信息被篡改而导致计算机设备遭受病毒等攻击的危险;而且,由于第一验证信息以及第二验证信息均可根据安装信息来获得,使得本发明的方法与硬件或安装信息的获取方式相脱离,适用面较广且实施简便。

[0196] 图 5 为图 4 所示的实施例中加密装置的一个优选实施例的结构示意图。本实施例中的加密装置 2 包括第一字符获取装置 21 与第一子加密装置 22。

[0197] 第一字符获取装置 21 根据所述全部或部分安装信息中第一预定位置的字符来获得字符信息。其中,所述第一预定位置为未被篡改的安装信息中预定字符信息所在的位置。优选地,第一预定位置包括但不限于:一个或多个预定文件、各个预定文件中或其文件名中的一个或多个预定位置、预定路径和 / 或预定排序位的文件、预定路径和 / 或预定排序位的文件中或其文件名中的一个或多个预定位置等。例如,预定文件 abc.txt 包含的全部内容信息,或者,包含的内容信息中第 12 至 15 个字符;又例如,预定文件夹 txb 下按文件名字符降序排序后第二位的文件中包含的全部信息;又例如,对安装信息中所有文件的文件大小进行升序排序后第十位的文件的文件名中的全部信息等。

[0198] 具体地,第一字符获取装置 21 直接根据其包含的用于限定字符获取位置的信息,或者,根据更改装置所加入的预定字符信息的第一预定位置信息,确定第一预定位置;并且,第一字符获取装置 21 直接将所述全部或部分安装信息中一个第一预定位置的字符作为完整的字符信息;或者,第一字符获取装置 21 由所述全部或部分安装信息中的多个第一预定位置分别获得多个字符,并将所获得的多个字符进行诸如组合、变换等处理,来获得字符信息。

[0199] 例如,第一字符获取装置 21 直接根据其包含的用于限定字符获取位置的信息,确定第一预定位置包括:1) 文件 wieng.txt 的第 2 至 4 个文件名字符;以及 2) 文件 xoing.doc 包含的内容中第 12 个字符以及第 45 个字符;接着,第一字符获取装置 21 访问文件 wieng.txt 以及 xoing.doc,获得文件 wieng.txt 的第 2 至 4 个文件名字符为“ien”,并获得文件 xoing.doc 包含的内容中第 12 和 45 个字符分别为“e”和“t”;接着,第一字符获取装置 21 将由 wieng.txt 文件名中获得的字符顺序颠倒,并与文件 xoing.doc 中获得的字符组合,获得字符信息“neiet”。

[0200] 又例如,更改装置将第一预定位置信息加入预定文件 location.txt 中,第一字符获取装置 21 访问预定文件 location.txt,获得更改装置加入的第一预定位置信息包括“文件路径:shig\pst\amaz.txt;字符位置:文件中第 15-21 个字符”,则第一字符获取装置 21 根据文件路径访问文件 amaz.txt,并将其中第 15-21 个字符作为完整的字符信息。

[0201] 需要说明的是,上述举例仅为更好地说明本发明的技术方案,而非对本发明的限制,本领域技术人员应该理解,任何获取所述全部或部分安装信息中第一预定位置的字符信息的实现方式,均应包含在本发明的范围内。

[0202] 接着,第一子加密装置 22 对字符信息进行预定加密处理,以获得所述第二验证信息。

[0203] 其中,第一子加密装置 22 对字符信息进行预定加密处理来获得第二验证信息的方式,与图 4 所示实施例中加密装置 2 对包含于全部或部分安装信息中的字符信息进行预定加密处理,以获得第二验证信息的方式相同或相似,并以引用的方式包含于此,不再赘述。

[0204] 由于安装信息经过被解析并添加诸如病毒等篡改处理后,由该经过篡改处理的安装信息中获取的第一预定位置的字符信息往往回不同于由未被篡改的安装信息中获取的预定位置的字符信息,由此,对由该经过篡改处理的安装信息中获取的第一预定位置的字符信息进行预定加密处理后,所获得的第二验证信息与第一验证信息匹配的概率就会大大降低,因此,根据本实施的方法,可进一步提高被篡改安装信息的检出率。

[0205] 图 6 为图 4 所示的实施例中第一获取装置的一个优选实施例的结构示意图。其中,本实施例的第一获取装置 1 包括第一子获取装置 11 以及第一处理装置 12。

[0206] 第一子获取装置 11 由所述全部或部分安装信息的第二预定位置获取待处理信息。

[0207] 其中,所述第二预定位置为未被篡改的安装信息中的待处理信息所在的位置。优选地,第二预定位置包括但不限于:一个或多个预定文件、各个预定文件中或其文件名中的一个或多个预定位置、预定路径和 / 或预定排序位的文件、预定路径和 / 或预定排序位的文件中或其文件名中的一个或多个预定位置等。

[0208] 具体地,第一子获取装置 11 由所述全部或部分安装信息中的一个第二预定位置处获得全部待处理信息;或者,第一子获取装置 11 由所述全部或部分安装信息中的多个第二预定位置处分别获得多个待处理信息。

[0209] 其中,第一子获取装置 11 由所述全部或部分安装信息的第二预定位置获取待处理信息的方式,与图 4 所示的实施例的第一获取装置 1 由预获取的全部或部分安装信息中直接获取第一验证信息的方式相同或相似,并以引用的方式包含于此,不再赘述。

[0210] 接着,第一处理装置 12 对所述待处理信息进行第一预定处理,以获得所述第一验证信息。

[0211] 其中,第一处理装置 12 对所述待处理信息进行第一预定处理的处理方式,与前述更改装置对第一验证信息进行第二预定处理的处理方式相匹配。例如,所述第二预定处理为拆分,则第一预定处理为合并;又例如,所述第二预定处理为加密,则第一预定处理为解密等等。优选地,第一预定处理的处理方式包括但不限于:合并、加密、解密、值的逻辑运算等等。

[0212] 例如,第一子获取装置 11 获取的两个待处理信息分别包括“0101”与“1011”,第一预定处理为求取两个待处理信息的异或值,则第一处理装置 12 求取“0101”与“1011”的异或值“1110”,以作为第一验证信息。

[0213] 又例如,第一预定处理为 MD5 处理,则第一处理装置 12 采用预定 MD5 算法,对第一子获取装置 11 获取的待处理信息进行加密处理,获得第一验证信息。

[0214] 再例如,第一预定处理为按序对多个待处理信息进行合并,则第一处理装置 12 将第一子获取装置 11 获得的三个待处理信息按照预定顺序进行合并,以将合并后的信息作

为第一验证信息等。

[0215] 需要说明的是,上述举例仅为更好地说明本发明的技术方案,而非对本发明的限制,本领域技术人员应该理解,对所述待处理信息进行第一预定处理,以获得所述第一验证信息的处理方式,由前述更改装置对待处理信息进行第二预定处理的处理方式来确定。

[0216] 作为一种优选方式,前述图 4、图 5 及图 6 所示的实施例中的第一获取装置 1 包括第二子获取装置(未予图示)、加密装置 2 包括第二子加密装置(未予图示),所述检测装置还包括第二获取装置(未予图示)及迭代装置(未予图示)。

[0217] 第二子获取装置根据预获取的部分安装信息来获得所述第一验证信息。其中,所述第二子获取装置根据预获取的部分安装信息来获得所述第一验证信息的方式,与图 4 或图 6 所示的实施例中第一获取装置 1 获得所述第一验证信息的方式相同或相似,在此不再赘述。

[0218] 优选地,第二子获取装置包括第五子获取装置(未予图示)以及第二处理装置(未予图示)。第五子获取装置由所述部分安装信息中的第二预定位置获取待处理信息;第二处理装置对所述待处理信息进行第一预定处理,以获得所述第一验证信息。其中,第五子获取装置由所述部分安装信息中的第二预定位置获取待处理信息,以及第二处理装置对所述待处理信息进行第一预定处理,以获得所述第一验证信息的方式,与图 6 所示的实施例中第一子获取装置 11 由第二预定位置获取待处理信息,以及第一处理装置 12 对所述待处理信息进行第一预定处理,以获得所述第一验证信息的方式相同或相似,在此不再赘述。

[0219] 第二子加密装置对包含于所述部分安装信息中的字符信息进行所述预定加密处理,以获得第二验证信息。其中,所述第二子加密装置对包含于所述部分安装信息中的字符信息进行所述预定加密处理来获得第二验证信息的方式,与图 4 或图 5 所示的实施例中的加密装置 2 获得第二验证信息的方式相同或相似,并以引用的方式包含于此,不再赘述。

[0220] 优选地,第二子加密装置包括第二字符获取装置(未予图示)以及第五子加密装置(未予图示)。第二字符获取装置获取所述部分安装信息中第一预定位置的字符信息;第五子加密装置对所述第一预定位置的字符信息进行预定加密处理,以获得所述第二验证信息。其中,第二字符获取装置获取所述部分安装信息中第一预定位置的字符信息,以及第五子加密装置对所述第一预定位置的字符信息进行所述预定加密处理,以获得所述第二验证信息的方式,与图 5 所示的实施例中第一字符获取装置 21 获取第一预定位置的字符信息,以及第一子加密装置 22 对所述第一预定位置的字符信息进行所述预定加密处理,以获得所述第二验证信息的方式相同或相似,并以引用的方式包含于此,不再赘述。

[0221] 接着,判断装置 3 执行图 4、图 5 或图 6 实施例中判断所述第一验证信息与所述第二验证信息是否匹配的操作,以判断第一验证信息与第二验证信息是否匹配的操作。

[0222] 当判断所述第一验证信息与所述第二验证信息匹配时,第二获取装置获取另一部分安装信息,并将所述另一部分安装信息作为所述部分安装信息。

[0223] 其中,所述第二获取装置获取另一部分安装信息的方式包括但不限于:1)所述第二获取装置触发自身所属第一计算机设备执行获取另一部分安装信息的操作;其中,所述第一计算机设备获取另一部分安装信息的获取方式与图 4 所示的实施例中在第一获取装置 1 获取第一验证信息之前所述第一计算机设备预获取部分安装信息的获取方式相同或相似,并以引用的方式包含于此,不再赘述;2)由已存储所述另一部分安装信息的装置或

设备提供给所述第一获取装置 1 等。

[0224] 需要说明的是,上述举例仅为更好地说明本发明的技术方案,而非对本发明的限制,本领域技术人员应该理解,任何获取另一部分安装信息的实现方式,均应包含在本发明的范围内。

[0225] 接着,迭代装置触发所述第二子获取装置与第二子加密装置,以使所述第二子获取装置、所述第二子加密装置、所述判断装置及所述第二获取装置重复执行操作,直至所述第二获取装置获取所述另一部分安装信息失败或所述判断装置判断所述第一验证信息与所述第二验证信息不匹配。

[0226] 其中,所述第二获取装置获取另一部分安装信息失败的情形包括但不限于:因已经获取全部安装信息而导致再次获取另一部分安装信息的操作失败、因无法再次访问提供所述另一部分安装信息的网站导致获取所述另一部分安装信息的操作失败、因提供所述另一部分安装信息的设备或装置发生故障导致获取所述另一部分安装信息的操作失败等等。

[0227] 需要说明的是,当所述第二获取装置获取另一部分安装信息失败后,所述第二获取装置可以将用于提醒安装信息下载未完成的提示信息呈现给用户,也可以在预定时间后继续获取所述另一部分安装信息的操作等;当所述判断装置 3 判断所述第一验证信息与所述第二验证信息不匹配,则所述第一执行装置 4 执行与所述全部或部分安装信息相关的相应处理的操作。

[0228] 根据本实施例的检测装置,可对安装信息进行分段验证,以提前判断安装信息是否可能被篡改。特别是在安装信息的信息量较大的情况下,可以避免花费大量时间下载安装信息后才能验证安装信息是否被篡改的情况。

[0229] 作为一种优选方式,本发明的检测装置还包括查询装置(未予图示),前述图 4、图 5 及图 6 所示的实施例中的第一获取装置 1 还包括第三子获取装置(未予图示)、加密装置 2 还包括第三子加密装置(未予图示)。

[0230] 查询装置根据所述安装信息的获取来源来在预定白名单中进行查询。

[0231] 其中,所述获取来源包括提供所述安装信息的装置、设备或网站的信息等。所述查询装置获取所述获取来源的方式包括但不限于:1) 将由所述安装信息中获取的所述安装信息的来源信息作为所述获取来源;2) 当所述查询装置所属第一计算机设备正在获取所述安装信息时,所述查询装置将所述第一计算机设备所获得的提供所述安装信息的网页的地址信息或设备的标识信息作为所述安装信息的获取来源等。

[0232] 需要说明的是,上述举例仅为更好地说明本发明的技术方案,而非对本发明的限制,本领域技术人员应该理解,任何获取所述安装信息的获取来源的方式的实现方式,均应包含在本发明的范围内。

[0233] 当未能在所述预定白名单中查询到所述获取来源时,第三子获取装置根据已获取的全部或部分安装信息来获得所述第一验证信息。其中,第三子获取装置根据已获取的全部或部分安装信息来获得所述第一验证信息的方式与图 4 或图 6 所示的实施例中第一获取装置根据已获取的全部或部分安装信息来获得所述第一验证信息的方式相同或相似,并以引用的方式包含于此,不再赘述。

[0234] 当未能在所述预定白名单中查询到所述获取来源时,所述第三子加密装置对包含

于所述全部或部分安装信息中的字符信息进行所述预定加密处理,以获得所述第二验证信息。其中,第三子加密装置对包含于所述全部或部分安装信息中的字符信息进行所述预定加密处理来获得所述第二验证信息的方式,与图 4 或图 6 所示的实施例中加密装置对包含于所述全部或部分安装信息中的字符信息进行所述预定加密处理来获得所述第二验证信息的方式相同或相似,并以引用的方式包含于此,不再赘述。

[0235] 需要说明的是,第三子获取装置执行根据已获取的全部或部分安装信息来获得所述第一验证信息的操作与第三子加密装置执行对包含于所述全部或部分安装信息中的字符信息进行所述预定加密处理,以获得所述第二验证信息的操作并无先后顺序。

[0236] 接着,判断装置 3 执行图 4、图 5 或图 6 所示实施例中判断所述第一验证信息与所述第二验证信息是否匹配的操作;当判断装置 3 判断判断第一验证信息与第二验证信息不匹配时,第一执行装置 4 执行图 4、图 5 或图 6 所示实施例中与所述全部或部分安装信息相关的相应处理的操作。

[0237] 根据本实施例的检测装置,无需再对由可信来源处获得的安装信息进行验证,减少了设备资源消耗。

[0238] 作为一种优选方式,前述图 4、图 5 及图 6 所示的实施例中的第一获取装置 1 还包括第四子获取装置(未予图示),加密装置 2 还包括第四子加密装置(未予图示)。

[0239] 当获得用户要求基于预获取的全部安装信息来执行安装操作的指令时,第四子获取装置根据所述全部安装信息来获得第一验证信息。其中,第四子获取装置根据预获取的全部安装信息来获得第一验证信息的方式,与图 4 或图 6 所示的实施例中第一获取装置 1 根据预获取的全部安装信息来获得第一验证信息的方式相同或相似,并以引用的方式包含于此,不再赘述。其中,所述第四子获取装置获得用户要求基于所述全部安装信息来执行安装操作的指令的方式包括但不限于:所述第四子获取装置通过接收诸如键盘、鼠标或触摸笔等人机交互设备发出的信息来获得用户要求基于所述全部安装信息来执行安装操作的指令等。

[0240] 当获得用户要求基于所述全部安装信息来执行安装操作的指令时,第四子加密装置对包含于所述全部安装信息中的字符信息进行所述预定加密处理,以获得所述第二验证信息。其中,第四子加密装置对包含于所述全部或部分安装信息中的字符信息进行所述预定加密处理来获得所述第二验证信息的方式,与图 4 或图 5 所示的实施例中加密装置 2 对包含于所述全部或部分安装信息中的字符信息进行所述预定加密处理来获得所述第二验证信息的方式相同或相似,并以引用的方式包含于此,不再赘述。

[0241] 需要说明的是,第四子获取装置执行根据所述全部安装信息来获得第一验证信息的操作与第四子加密装置执行对包含于所述全部安装信息中的字符信息进行所述预定加密处理来获得所述第二验证信息的操作并无先后顺序。

[0242] 根据本实施例的检测装置,仅在用户要求基于安装信息来进行安装操作时,才启动验证处理,避免了用户因突然收到安装信息可能被篡改的通知而产生突兀感。

[0243] 对于本领域技术人员而言,显然本发明不限于上述示范性实施例的细节,而且在不背离本发明的精神或基本特征的情况下,能够以其他的具体形式实现本发明。因此,无论从哪一点来看,均应将实施例看作是示范性的,而且是非限制性的,本发明的范围由所附权利要求而不是上述说明限定,因此旨在将落在权利要求的等同要件的含义和范围内的所有

变化涵括在本发明内。不应将权利要求中的任何附图标记视为限制所涉及的权利要求。此外，显然“包括”一词不排除其他单元或步骤，单数不排除复数。系统权利要求中陈述的多个单元或装置也可以由一个单元或装置通过软件或者硬件来实现。第一，第二等词语用来表示名称，而并不表示任何特定的顺序。

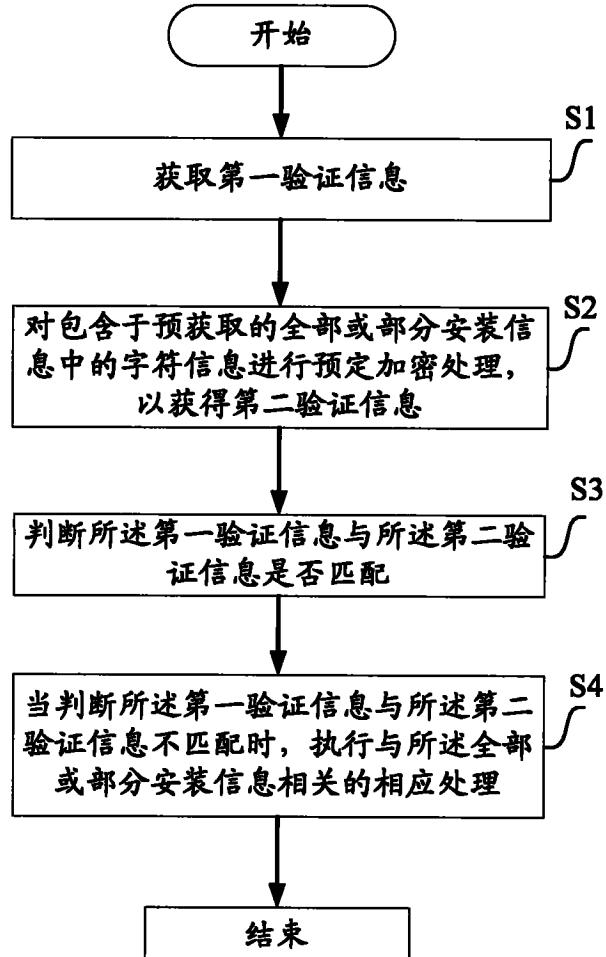


图 1

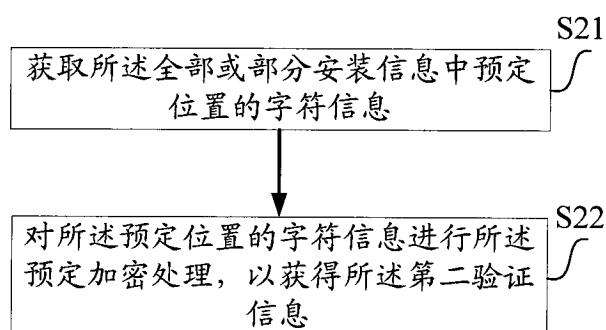


图 2

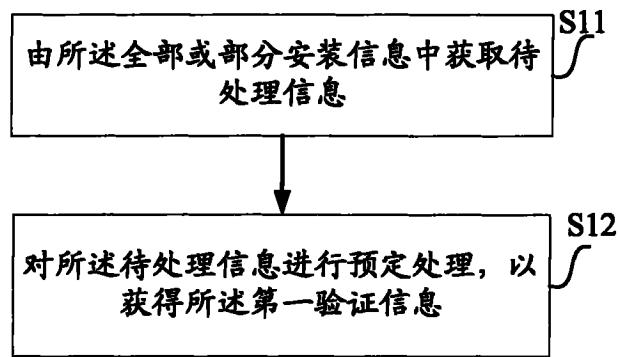


图 3

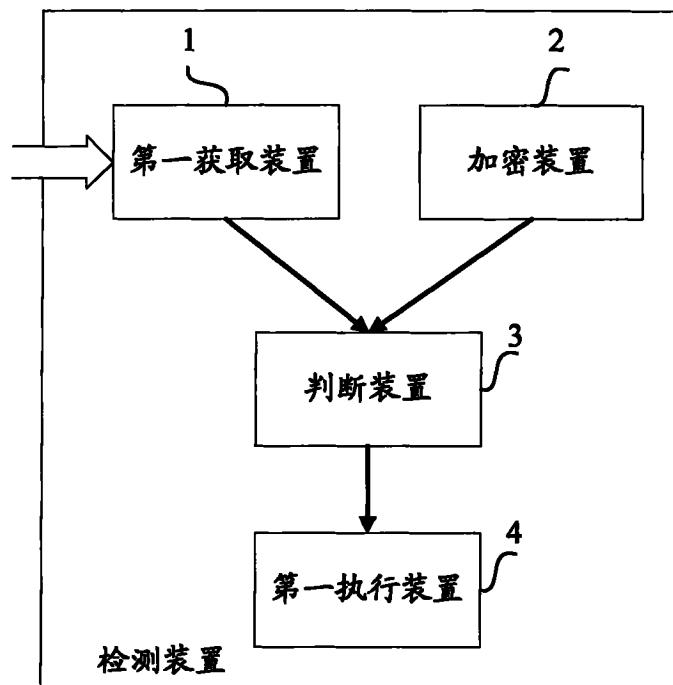


图 4

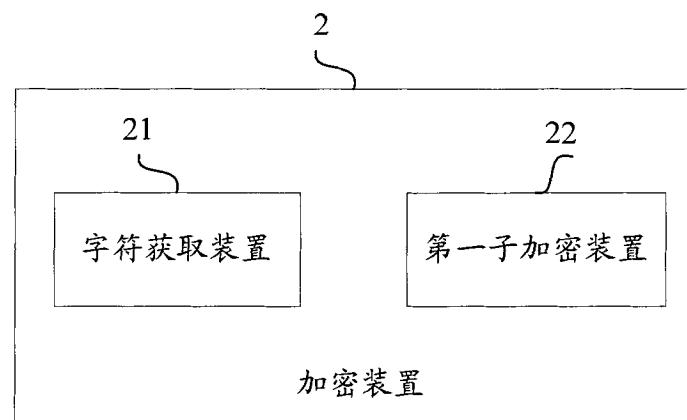


图 5

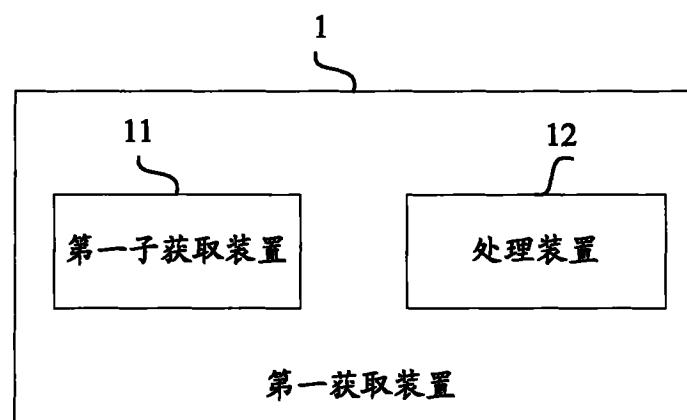


图 6