(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 106295263 A
(43)申请公布日 2017.01.04

(21)申请号 201510268570.3

(22)申请日 2015.05.22

(71)申请人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦法务部

(72)发明人 陈华 卫伟 张家明

(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
代理人 韩辉峰 李丹

(51)Int.Cl.
G06F 21/14(2013.01)
G06F 21/60(2013.01)

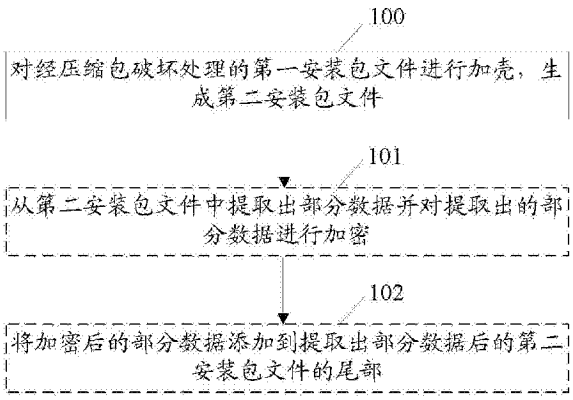
权利要求书2页 说明书4页 附图1页

(54)发明名称

一种实现应用加固的方法及装置

(57)摘要

本发明公开了一种实现应用加固的方法及装置，包括：对经压缩包破坏处理的第一安装包文件进行加壳，生成第二安装包文件，以对应用进行加固。本发明方法对经压缩包破坏处理的第一安装包文件进行加壳，避免了压缩包破坏的第一安装包文件被压缩文件修复工具修复导致加固保护消失；通过对压缩包破坏的第一安装包文件进行加壳，避免了在执行完壳代码跳转到安装包的原始入口后，被保护安装包的数据都暴露在内存中，实现了应用的加固，提高了安装包文件的安全性。进一步地，通过从第二安装包文件中提取出部分数据并对提取出的部分数据进行加密，放置于第二安装包文件的尾部的处理，加大了安装包文件的保护力度，进一步提高了安装包文件的安全性。



CN 106295263 A

1.一种实现应用加固的方法，其特征在于，包括：

对经压缩包破坏处理的第一安装包文件进行加壳，生成第二安装包文件，以对应用进行加固。

2.根据权利要求1所述的方法，其特征在于，所述生成第二安装包文件之后，该方法还包括：

从所述第二安装包文件中提取出部分数据并对提取出的部分数据进行加密；

将加密后的部分数据添加到所述提取出部分数据后的第二安装包文件的尾部。

3.根据权利要求2所述的方法，其特征在于，所述部分数据为：所述第二安装包文件中任意的可执行指令和/或动态链接表和/或段信息和/或节信息。

4.根据权利要求2所述的方法，其特征在于，所述提取出部分数据时，该方法还包括：

记录所述部分数据在所述壳保护文件中的位置，以获得提取位置信息。

5.根据权利要求4所述的方法，其特征在于，所述加密提取出的部分数据之前，该方法还包括：

将所述提取位置信息添加到所述提取出的部分数据中的预设位置。

6.根据权利要求5所述的方法，其特征在于，将加密后的部分数据添加到所述提取出部分数据后的第二安装包文件的尾部时，该方法还包括：

记录获得添加到所述提取出部分数据后的第二安装包文件的尾部的所述加密后的部分数据的添加位置信息。

7.根据权利要求2～6任一项所述的方法，其特征在于，所述对提取出的部分数据进行加密具体包括：

对所述提取部分数据通过消息摘要算法第五版MD5进行加密。

8.根据权利要求6所述的方法，其特征在于，所述安装包为安卓安装包APK。

9.根据权利要求8所述的方法，其特征在于，在进行APK安装时，该方法还包括：

将所述加密后的部分数据还原为所述第二安装包文件；

在执行完壳代码跳转到APK的原始入口后，通过所述压缩包破坏的文件进行APK安装。

10.根据权利要求9所述的方法，其特征在于，所述还原加密后的部分数据为第二安装包文件具体包括：

通过所述添加位置信息读取所述加密后的部分数据；

解密所述加密后的部分数据，从所述预设位置中读取所述提取位置信息；

根据读取的所述提取位置信息，将解密的部分数据还原为所述第二安装包文件。

11.一种实现应用加固的装置，其特征在于，至少包括预处理单元和加固单元，其中，

预处理单元，对安装包文件进行压缩包破坏处理；

加固单元，用于对经压缩包破坏处理的第一安装包文件进行加壳，生成第二安装包文件，以对应用进行加固。

12.根据权利要求11所述的装置，其特征在于，该装置还包括提取处理单元，用于所述生成第二安装包文件之后，从所述第二安装包文件中提取出部分数据并对提取出的部分数据进行加密；

将获得的加密后的部分数据添加到所述提取出部分数据后的第二安装包文件的尾部。

13.根据权利要求12所述的装置，其特征在于，该装置还包括记录单元，用于所述提取

出所述部分数据时，记录加密后的部分数据在所述壳保护文件中的位置，以获得提取位置信息。

14. 根据权利要求 13 所述的装置，其特征在于，该装置添加处理单元，用于所述加密提取出的部分数据之前，将所述提取位置信息添加到所述提取出的部分数据中的预设位置。

15. 根据权利要求 14 所述的装置，其特征在于，所述记录单元还用于，将所述加密后的部分数据添加到所述提取出部分数据后的第二安装包文件的尾部时，记录获得添加到所述提取出部分数据后的第二安装包文件的尾部的所述加密后的部分数据的添加位置信息。

一种实现应用加固的方法及装置

技术领域

[0001] 本发明涉及应用安全领域，尤指一种实现应用加固的方法及装置。

背景技术

[0002] 随着智能终端的发展，终端应用的数量得到快速的膨胀，用户通过终端应用进行越来越多的日常事务处理，终端应用安全成为开发者和用户都关注的技术问题。为了提高终端应用的安全，技术人员对终端应用进行处理，其中，包含对安装包的加固。以安卓(Android)平台为例，安卓系统是移动终端普及最广的操作系统之一，Android平台以开放性吸引众多开发者、以免费性赢得大量的用户。越来越多的Android应用被人们用来处理如收发邮件、电子支付、社交通信等日常事务。Android应用在使用过程中不可避免的需要访问存储用户的账号、密码等数据，因而成为恶意软件的攻击对象。随着Android应用范围的增大，威胁范围越来越广，威胁程度也在加深。为了提高Android应用的安全性，开发人员对Android安装包(APK)进行了加固处理，通过加固处理，可以提高Android应用的安全，常用的加固方法有：伪加密、压缩包破坏、代码混淆、签名验证等。

[0003] 伪加密是通过java代码对APK压缩文件进行伪加密。压缩包破坏通过在标志尾添加其他数据，由于Android系统对APK的识别是将APK当作压缩文件，从标志头到标志尾的逻辑进行识别的，如果在标志尾添加其他数据，则APK会被判断为被破坏，在对压缩包破坏的APK进行解压、查看或用反编译处理时，均会提示文件已损坏，压缩包破坏与伪加密类似，但标志尾添加其他数据的APK不会影响其在Android系统的正常运行和安装。代码混淆主要是干扰逆向工作人员的分析，加大破解者对软件的分析难度，达到混淆视听的效果，经过混淆后的代码在反汇编或者反编译后，会出现程序间交叉引用异常复杂，从而达到加固APK的目的。签名验证通过与APK绑定，实现APK的加固。

[0004] 上述加固方法，由于在Android4.2之后推出的系统，修改了签名验证的方式导致无法安装伪加密的APK；通过采用压缩文件修复工具，会将APK压缩包破坏方法添加到标志尾的其他数据进行修复，使APK加固保护消失。经过混淆后的代码在反汇编或者反编译后，有可能与反射发生冲突，且代码混淆方法只是增大破解难度，并不能真正阻止反向工程，无法达到真正的保护目的。签名验证存在APK被反编译后签名会自动消失，APK保护也会同时失效。综上，现有的应用加固方法，仍存在安全问题，影响移动终端的安全应用和发展。

发明内容

[0005] 为了解决上述对应用加固方法存在的安全问题，本发明提供一种实现应用加固的方法及装置，能够加固应用，提高应用安全。

[0006] 为了达到本发明目的，本发明提供了一种实现应用加固的方法，包括：

[0007] 对经压缩包破坏处理的第一安装包文件进行加壳，生成第二安装包文件，以对应用进行加固。

[0008] 进一步地，生成第二安装包文件之后，该方法还包括：

[0009] 从所述第二安装包文件中提取出部分数据并对提取出的部分数据进行加密；

[0010] 将加密后的部分数据添加到所述提取出部分数据后的第二安装包文件的尾部。

[0011] 进一步地，部分数据为：所述第二安装包文件中任意的可执行指令和/或动态链接表和/或段信息和/或节信息。

[0012] 进一步地，提取出部分数据时，该方法还包括：

[0013] 记录所述部分数据在所述壳保护文件中的位置，以获得提取位置信息。

[0014] 进一步地，加密提取出的部分数据之前，该方法还包括：

[0015] 将所述提取位置信息添加到所述提取出的部分数据中的预设位置。

[0016] 进一步地，将加密后的部分数据添加到所述提取出部分数据后的第二安装包文件的尾部时，该方法还包括：

[0017] 记录获得添加到所述提取出部分数据后的第二安装包文件的尾部的所述加密后的部分数据的添加位置信息。

[0018] 进一步地，对提取出的部分数据进行加密具体包括：

[0019] 对所述提取部分数据通过消息摘要算法第五版 MD5 进行加密。

[0020] 进一步地，安装包为安卓安装包 APK。

[0021] 进一步地，在进行 APK 安装时，该方法还包括：

[0022] 将所述加密后的部分数据还原为所述第二安装包文件；

[0023] 在执行完壳代码跳转到 APK 的原始入口后，通过所述压缩包破坏的文件进行 APK 安装。

[0024] 进一步地，所述还原加密后的部分数据为第二安装包文件具体包括：

[0025] 通过所述添加位置信息读取所述加密后的部分数据；

[0026] 解密所述加密后的部分数据，从所述预设位置中读取所述提取位置信息；

[0027] 根据读取的所述提取位置信息，将解密的部分数据还原为所述第二安装包文件。

[0028] 另一方面，本申请还提供一种实现应用加固的装置，至少包括预处理单元和加固单元，其中，

[0029] 预处理单元，对安装包文件进行压缩包破坏处理；

[0030] 加固单元，用于对经压缩包破坏处理的第一安装包文件进行加壳，生成第二安装包文件，以对应用进行加固。

[0031] 进一步地，该装置还包括提取处理单元，用于所述生成第二安装包文件之后，从所述第二安装包文件中提取出部分数据并对提取出的部分数据进行加密；

[0032] 将获得的加密后的部分数据添加到所述提取出部分数据后的第二安装包文件的尾部。

[0033] 进一步地，该装置还包括记录单元，用于所述提取出所述部分数据时，记录加密后的部分数据在所述壳保护文件中的位置，以获得提取位置信息。

[0034] 进一步地，该装置添加处理单元，用于所述加密提取出的部分数据之前，将所述提取位置信息添加到所述提取出的部分数据中的预设位置。

[0035] 进一步地，所述记录单元还用于，将所述加密后的部分数据添加到所述提取出部分数据后的第二安装包文件的尾部时，记录获得添加到所述提取出部分数据后的第二安装包文件的尾部的所述加密后的部分数据的添加位置信息。

[0036] 与现有技术相比，本申请技术方案包括：对经压缩包破坏处理的第一安装包文件进行加壳，生成第二安装包文件，以对应用进行加固。本发明方法对经压缩包破坏处理的第一安装包文件进行加壳，避免了压缩包破坏的第一安装包文件被压缩文件修复工具修复时导致加固保护消失的问题；通过对压缩包破坏的第一安装包文件进行加壳，避免了在执行完壳代码跳转到安装包的原始入口后，被保护安装包的数据都暴露在内存中，实现了应用的加固，提高了安装包文件的安全性。

[0037] 进一步地，通过从第二安装包文件中提取出部分数据并对提取出的部分数据进行加密，放置于第二安装包文件的尾部的处理，加大了安装包文件的保护力度，进一步提高了安装包文件的安全性。

附图说明

[0038] 此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0039] 图 1 为本发明实现应用加固的方法的流程图；

[0040] 图 2 为本发明实现应用加固的装置的结构框图。

具体实施方式

[0041] 为使本发明的目的、技术方案和优点更加清楚明白，下文中将结合附图对本发明的实施例进行详细说明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互任意组合。

[0042] 图 1 为本发明实现应用加固的方法的流程图，如图 1 所示，包括：

[0043] 步骤 100、对经压缩包破坏处理的第一安装包文件进行加壳，生成第二安装包文件，以对应用进行加固。

[0044] 需要说明的是，对安装包文件进行压缩包破坏处理属于本领域技术人员的惯用技术手段，在此不再赘述。加壳是指在压缩包破坏处理的第一安装包文件中插入一段代码，在安装过程中，安装文件的入口点即安装包执行的第一条指令指向壳代码，经过加壳处理的软件在运行时会首先进入到壳代码中，在壳代码中把被压缩包破坏处理的第一安装包文件还原，然后再根据压缩包破坏处理的第一安装包文件进行按照。通过加壳可以减小压缩包破坏处理的第一安装包文件体积，便于传输，提高执行效率。

[0045] 生成第二安装包文件之后，该方法还包括：

[0046] 步骤 101、从第二安装包文件中提取出部分数据并对提取出的部分数据进行加密。

[0047] 部分数据为：第二安装包文件中任意的可执行指令和 / 或动态链接表和 / 或段信息和 / 或节信息。

[0048] 对提取出的部分数据进行加密具体包括：

[0049] 对提取部分数据通过消息摘要算法第五版 (MD5) 进行加密。

[0050] 提取出部分数据时，本发明方法还包括：

[0051] 记录部分数据在壳保护文件中的位置，以获得提取位置信息。

[0052] 加密提取出的部分数据之前，本发明方法还包括：

[0053] 将提取位置信息添加到提取出的部分数据中的预设位置。

[0054] 步骤102、将加密后的部分数据添加到提取出部分数据后的第二安装包文件的尾部。

[0055] 将加密后的部分数据添加到提取出部分数据后的第二安装包文件的尾部时，本发明方法还包括：

[0056] 记录获得添加到提取出部分数据后的第二安装包文件的尾部的加密后的部分数据的添加位置信息。

[0057] 本发明安装包为安卓安装包(APK)。

[0058] 在进行APK安装时，本发明方法还包括：

[0059] 将加密后的部分数据还原为第二安装包文件；

[0060] 在执行完壳代码跳转到APK的原始入口后，通过压缩包破坏的文件进行APK安装。

[0061] 还原加密后的部分数据为第二安装包文件具体包括：

[0062] 通过添加位置信息读取加密后的部分数据；

[0063] 解密加密后的部分数据，从预设位置中读取提取位置信息；

[0064] 根据读取的提取位置信息，将解密的加密后的部分数据还原为第二安装包文件。

[0065] 本发明方法对经压缩包破坏处理的第一安装包文件进行加壳，避免了压缩包破坏的第一安装包文件被压缩文件修复工具修复导致加固保护消失；通过对压缩包破坏的第一安装包文件进行加壳，避免了在执行完壳代码跳转到安装包的原始入口后，被保护安装包的数据都暴露在内存中，实现了应用的加固，提高了安装包文件的安全性。进一步地，通过从第二安装包文件中提取出部分数据并对提取出的部分数据进行加密，放置于第二安装包文件的尾部的处理，加大了安装包文件的保护力度，进一步提高了安装包文件的安全性。

[0066] 图2为本发明实现应用加固的装置的结构框图，如图2所示，至少包括预处理单元和加固单元，其中，

[0067] 预处理单元，对安装包文件进行压缩包破坏处理；

[0068] 加固单元，用于对经压缩包破坏处理的第一安装包文件进行加壳，生成第二安装包文件，以对应用进行加固。

[0069] 本发明装置还包括提取处理单元，用于生成第二安装包文件之后，从第二安装包文件中提取出部分数据并对提取出的部分数据进行加密；

[0070] 将加密后的部分数据添加到提取出部分数据后的第二安装包文件的尾部。

[0071] 本发明装置还包括记录单元，用于提取出部分数据时，记录部分数据在壳保护文件中的位置，以获得提取位置信息。

[0072] 记录单元还用于，将加密后的部分数据添加到提取出部分数据后的第二安装包文件的尾部时，记录获得添加到提取出部分数据后的第二安装包文件的尾部的加密后的部分数据的添加位置信息。

[0073] 本发明装置还包括添加处理单元，用于加密提取出的部分数据之前，将提取位置信息添加到提取出的部分数据中的预设位置。

[0074] 虽然本发明所揭露的实施方式如上，但所述的内容仅为便于理解本发明而采用的实施方式，并非用以限定本发明。任何本发明所属领域内的技术人员，在不脱离本发明所揭露的精神和范围的前提下，可以在实施的形式及细节上进行任何的修改与变化，但本发明的专利保护范围，仍须以所附的权利要求书所界定的范围为准。

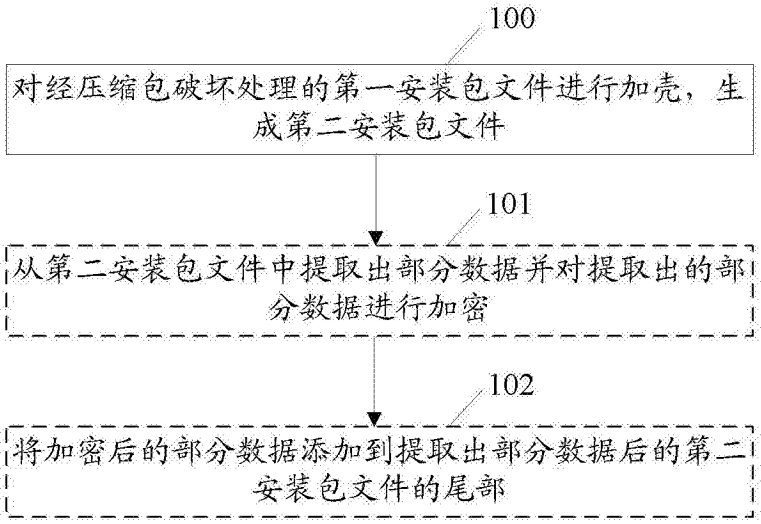

100
对经压缩包破坏处理的第一安装包文件进行加壳，生成第二安装包文件
101
从第二安装包文件中提取出部分数据并对提取出的部分数据进行加密
102
将加密后的部分数据添加到提取出部分数据后的第二安装包文件的尾部

图 1

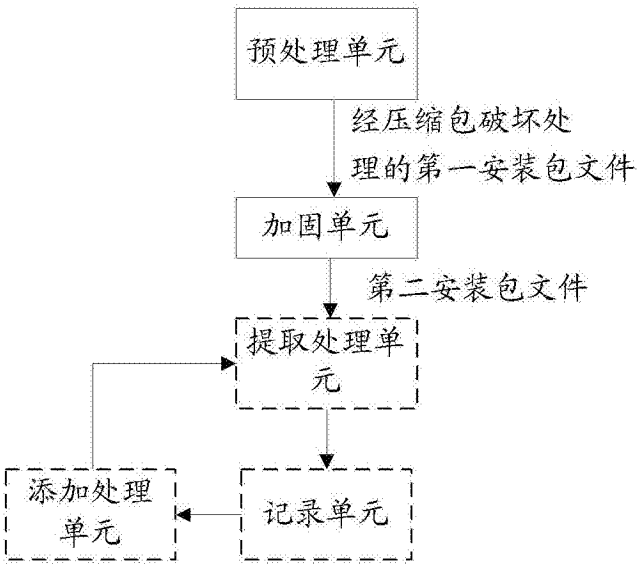

预处理单元
经压缩包破坏处理的第一安装包文件
加固单元
第二安装包文件
提取处理单元
添加处理单元
记录单元

图 2