(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 106295262 B
(45)授权公告日 2021.08.03

(21)申请号 201510252505.1

(22)申请日 2015.05.18

(65)同一申请的已公布的文献号
申请公布号 CN 106295262 A

(43)申请公布日 2017.01.04

(73)专利权人 腾讯科技(深圳)有限公司
地址 518000 广东省深圳市福田区振兴路赛格科技园2栋东403室

(72)发明人 蒋鑫 蒋宁波

(74)专利代理机构 深圳翼盛智成知识产权事务所(普通合伙) 44300
代理人 黄威

(51)Int.Cl.
G06F 21/14(2013.01)
G06F 21/53(2013.01)

(56)对比文件
CN 101122938 A,2008.02.13
CN 101520800 A,2009.09.02
CN 103593617 A,2014.02.19
US 2013013270 A1,2013.01.10
张逢喆.公共云计算环境下用户数据的隐私性与安全性保护.《中国博士学位论文全文数据库 信息科技辑》.2012,第2012卷(第1期),

审查员 岳孟果

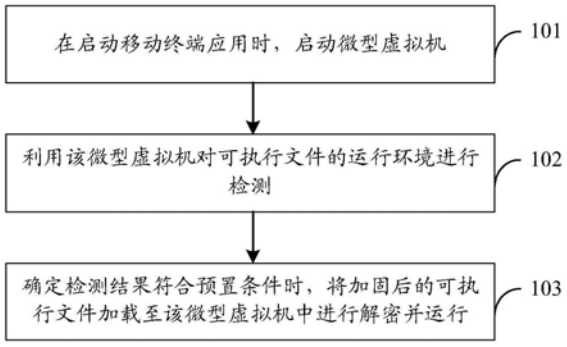
权利要求书2页 说明书9页 附图3页

(54)发明名称

一种可执行文件的处理方法、装置和系统

(57)摘要

本发明实施例公开了一种可执行文件的处理方法、装置和系统;本发明实施例采用在启动移动终端应用时,启动微型虚拟机,利用该微型虚拟机对可执行文件的运行环境进行检测,并在确定检测结果符合预置条件时,将加固后的可执行文件加载至该微型虚拟机中进行解密并运行;该方案可以更好地对代码进行加固,在保护代码,提高数据安全性的同时,提高运行效率。



CN 106295262 B

1.一种可执行文件的处理方法,其特征在于,包括:

在启动移动终端应用时,启动微型虚拟机,并对所述微型虚拟机设置最高优先运行权;

利用该微型虚拟机对微型虚拟机自身的完整性进行检测;

利用所述微型虚拟机对可执行文件的运行环境进行检测;

确定检测结果符合预置条件时,将加固后的可执行文件加载至所述微型虚拟机中,并确定所述加固后的可执行文件中加密索引的位置;

根据确定的位置获取相应的加密索引,并在所述微型虚拟机中对加密索引进行解密,得到解密后索引;

在所述微型虚拟机中,根据解密后索引还原所述可执行文件的代码并在微型虚拟机中运行还原后代码。

2.根据权利要求1所述的方法,其特征在于,还包括:

获取可执行文件中需要加固的代码的索引;

对所述需要加固的代码的索引进行加密,得到加密索引;

将加密索引添加至所述可执行文件中的相应位置,得到加固后的可执行文件。

3.根据权利要求2所述的方法,其特征在于,所述获取可执行文件中需要加固的代码的索引,包括:

获取移动终端应用提交的关于可执行文件的加固请求;

根据所述加固请求扫描所述移动终端应用的可执行文件,以获取需要加固的代码;

根据预置的虚拟机特性获取所述需要加固的代码的索引。

4.根据权利要求1至3任一项所述的方法,其特征在于,所述利用所述微型虚拟机对可执行文件的运行环境进行检测,包括:

利用所述微型虚拟机对微型虚拟机自身的完整性进行检测;以及,

利用所述微型虚拟机对可执行文件的运行环境的安全性进行检测;

若完整性检测通过且运行环境为安全,则确定检测结果符合预置条件;

若完整性检测不通过或运行环境不安全,则确定检测结果不符合预置条件。

5.一种可执行文件的处理装置,其特征在于,包括:

启动单元,用于在启动移动终端应用时,启动微型虚拟机,并对所述微型虚拟机设置最高优先运行权;

检测单元,用于利用该微型虚拟机对微型虚拟机自身的完整性进行检测;利用所述微型虚拟机对可执行文件的运行环境进行检测;

处理单元,用于确定检测结果符合预置条件时,将加固后的可执行文件加载至所述微型虚拟机中,并确定所述加固后的可执行文件中加密索引的位置;根据确定的位置获取相应的加密索引,并在所述微型虚拟机中对加密索引进行解密,得到解密后索引;在所述微型虚拟机中,根据解密后索引还原所述可执行文件的代码并在微型虚拟机中运行还原后代码。

6.根据权利要求5所述的装置,其特征在于,还包括获取单元、加密单元和添加单元;

所述获取单元,用于获取可执行文件中需要加固的代码的索引;

所述加密单元,用于对所述需要加固的代码的索引进行加密,得到加密索引;

所述添加单元,用于将加密索引添加至所述可执行文件中的相应位置,得到加固后的

可执行文件。

7.根据权利要求6所述的装置,其特征在于,

所述获取单元,具体用于获取移动终端应用提交的关于可执行文件的加固请求,根据所述加固请求扫描所述移动终端应用的可执行文件,以获取需要加固的代码,根据预置的虚拟机特性获取所述需要加固的代码的索引。

8.根据权利要求5至7任一项所述的装置,其特征在于,所述检测单元,具体用于:

利用所述微型虚拟机对微型虚拟机自身的完整性进行检测;以及,

利用所述微型虚拟机对可执行文件的运行环境的安全性进行检测;

若完整性检测通过且运行环境为安全,则确定检测结果符合预置条件;

若完整性检测不通过或运行环境不安全,则确定检测结果不符合预置条件。

9.一种可执行文件的处理系统,其特征在于,包括微型虚拟机和权利要求5至8任一项所述的可执行文件的处理装置,其中:

所述微型虚拟机,用于在所述可执行文件的处理装置的控制下启动,并在所述可执行文件的处理装置的控制下,对加载在本微型虚拟机中的加固后的可执行文件进行解密并运行。

10.一种存储介质,其内存储有处理器可执行指令,所述指令由一个或一个以上处理器加载,以执行如权利要求1至4中任一项所述的可执行文件的处理方法。

11.一种电子设备,包括处理器和存储器,所述存储器储存有计算机程序,所述处理器通过调用所述计算机程序,用于执行如权利要求1至4中任一的可执行文件的处理方法。

一种可执行文件的处理方法、装置和系统

技术领域

[0001] 本发明涉及通信技术领域，具体涉及一种可执行文件的处理方法、装置和系统。

背景技术

[0002] 在移动终端高度普及的今天，基于种种目的，大量的移动终端应用被破解，并进行反编译等操作，从而构建出大量的山寨应用的安装包，影响用户对移动终端应用的使用；更甚者，这些山寨应用的安装包中还可能会植入广告插件或恶意指令等，对用户数据与财产带来严重的安全隐患，为此，如何防止移动终端应用被破解和反编译，对于数据安全具有重大意义。

[0003] 由于移动终端应用的指令多数都是编译在可执行文件中，比如，安卓(Android)系统的dex文件中，因此，为了防止可执行文件被反编译，在现有技术中，一般会对可执行文件进行整体加密，然后在运行时，才在内存中对其进行解密并重组成系统所需的文件，比如odex文件。

[0004] 在对现有技术的研究和实践过程中，本发明的发明人发现，虽然现有技术可在一定程度上降低可执行文件被反编译的几率，但是，由于解密后内存中存在原始代码，若反编译者从内存中把原始代码拷贝出来，一样可以达到反编译的目的，因此，现有方案对于代码的保护力度并不够；而且，由于运行时需要解密大量的数据，所以，其运行效率也较低。

发明内容

[0005] 本发明实施例提供一种可执行文件的处理方法、装置和系统，可以更好地对代码进行加固，在保护代码，提高数据安全性的同时，提高运行效率。

[0006] 本发明实施例提供一种可执行文件的处理方法，包括：

[0007] 在启动移动终端应用时，启动微型虚拟机；

[0008] 利用所述微型虚拟机对可执行文件的运行环境进行检测；

[0009] 确定检测结果符合预置条件时，将加固后的可执行文件加载至所述微型虚拟机中进行解密并运行。

[0010] 相应的，本发明实施例还提供一种可执行文件的处理装置，包括：

[0011] 启动单元，用于在启动移动终端应用时，启动微型虚拟机；

[0012] 检测单元，用于利用所述微型虚拟机对可执行文件的运行环境进行检测；

[0013] 处理单元，用于确定检测结果符合预置条件时，将加固后的可执行文件加载至所述微型虚拟机中进行解密并运行。

[0014] 此外，本发明实施例还提供一种可执行文件的处理系统，包括微型虚拟机和本发明实施例所提供的任一种可执行文件的处理装置，其中：

[0015] 所述微型虚拟机，用于在所述可执行文件的处理装置的控制下启动，并在所述可执行文件的处理装置的控制下，对加载在本微型虚拟机中的加固后的可执行文件进行解密并运行。

[0016] 本发明实施例采用在启动移动终端应用时，启动微型虚拟机，利用该微型虚拟机对可执行文件的运行环境进行检测，并在确定检测结果符合预置条件时，将加固后的可执行文件加载至该微型虚拟机中进行解密并运行；由于本方案在进行解密和运行代码之前，均会对运行环境进行检测，以保证运行环境的安全性，因此，可以更好地保护代码，提高数据安全性；而且，由于代码的解密和运行是在指定的微型虚拟机中进行的，因此，相对于现有技术只能在内存中进行解密和运行的方案而言，可以避免受其他进程的影响，提高其运行效率。

附图说明

[0017] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0018] 图1是本发明实施例提供的可执行文件的处理方法的流程示意图；

[0019] 图2a是本发明实施例提供的可执行文件的处理方法中的加固流程图；

[0020] 图2b是本发明实施例提供的可执行文件的处理方法中的运行流程图；

[0021] 图3a是本发明实施例提供的可执行文件的处理装置的结构示意图；

[0022] 图3b是本发明实施例提供的可执行文件的处理装置的另一结构示意图；

[0023] 图4是本发明实施例提供的移动终端的结构示意图。

具体实施方式

[0024] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0025] 本发明实施例提供一种可执行文件的处理方法、装置和系统。以下将分别进行详细说明。

[0026] 实施例一、

[0027] 本实施例将从可执行文件的处理装置的角度进行描述，该可执行文件的处理装置具体可以集成在移动终端等设备中，该移动终端具体可以为手机或平板电脑等。

[0028] 一种可执行文件的处理方法，包括：在启动移动终端应用时，启动微型虚拟机；利用该微型虚拟机对可执行文件的运行环境进行检测；确定检测结果符合预置条件时，将加固后的可执行文件加载至该微型虚拟机中进行解密并运行。

[0029] 如图1所示，该可执行文件的处理方法的流程具体可以如下：

[0030] 101、在启动移动终端应用时，启动微型虚拟机。

[0031] 例如，以安卓系统为例，具体可以利用安卓系统原有dalvik(一种用于Android平台的Java虚拟机)的解释运行的特性，来指定本移动终端专属的微型虚拟机，使得该微型虚拟机可以具有加固后的可执行文件运行前的最高优先运行权，即在加固后的可执行文件运行前优先运行微型虚拟机，这样，在启动移动终端应用时，便可以启动微型虚拟机。

[0032] 102、利用该微型虚拟机对可执行文件的运行环境进行检测。

[0033] 其中，对该运行环境的检测包括对微型虚拟机自身的完整性的检测，以及对运行环境的安全性的检测，即步骤“利用该微型虚拟机对可执行文件的运行环境进行检测”具体可以如下：

[0034] 利用该微型虚拟机对微型虚拟机自身的完整性进行检测；以及，

[0035] 利用该微型虚拟机对可执行文件的运行环境的安全性进行检测；

[0036] 若完整性检测通过且运行环境为安全，则确定检测结果符合预置条件；

[0037] 若完整性检测不通过或运行环境不安全，则确定检测结果不符合预置条件。

[0038] 其中，完整性检测和安全性检测的执行步骤可以不分先后，在此不再赘述。

[0039] 103、确定检测结果符合预置条件时，将加固后的可执行文件加载至该微型虚拟机中进行解密并运行。

[0040] 例如，可以将加固后的可执行文件加载至该微型虚拟机中，并确定该加固后的可执行文件中加密代码的位置，根据确定的位置获取相应的加密索引，并在该微型虚拟机中对加密索引进行解密，得到解密后索引，然后，在该微型虚拟机中，根据解密后索引还原该可执行文件的代码并运行还原后代码。

[0041] 其中，加固后的可执行文件指的是加密后的可执行文件，加固的方式可以有多种，例如，具体可以如下：

[0042] (1)获取可执行文件中需要加固的代码的索引。

[0043] 例如，具体可以获取移动终端应用提交的关于可执行文件的加固请求，根据该加固请求扫描该移动终端应用的可执行文件，以获取需要加固的代码，然后根据预置的虚拟机特性获取该需要加固的代码的索引。

[0044] (2)对该需要加固的代码的索引进行加密，得到加密索引。

[0045] 其中，加密的方式可以有多种，具体可以根据实际应用的需求进行设置，在此不再赘述。

[0046] (3)将加密索引添加至该可执行文件中的相应位置，得到加固后的可执行文件。

[0047] 由上可知，本实施例采用在启动移动终端应用时，启动微型虚拟机，利用该微型虚拟机对可执行文件的运行环境进行检测，并在确定检测结果符合预置条件时，将加固后的可执行文件加载至该微型虚拟机中进行解密并运行；由于本方案在进行解密和运行代码之前，均会对运行环境进行检测，以保证运行环境的安全性，因此，可以更好地保护代码，提高数据安全性；而且，由于代码的解密和运行是在指定的微型虚拟机中进行的，因此，相对于现有技术只能在内存中进行解密和运行的方案而言，可以避免受其他进程的影响，提高其运行效率，且兼容性更优。

[0048] 实施例二、

[0049] 根据实施例一所描述的方法，以下将举例作进一步详细说明。

[0050] 在本实施例中，将以安卓系统为例进行说明。其中，该可执行文件的处理装置具体可以集成在移动终端中，简称为处理装置，而该可执行文件具体可以为dex文件等。

[0051] 其中，该可执行文件的处理方法的流程包括可执行文件的加固流程和运行流程，以下将分别进行详细说明。

[0052] (1)加固；

[0053] 如图2a所示，该可执行文件的加固方法的具体流程可以如下：

[0054] A201、处理装置获取移动终端应用提交的关于可执行文件的加固请求，比如，关于dex文件的加固请求。

[0055] A202、处理装置根据该加固请求扫描该移动终端应用的可执行文件，比如扫描该移动终端应用的dex文件，以获取需要加固的代码。

[0056] A203、处理装置根据安卓系统的虚拟机特性获取该需要加固的代码的索引。

[0057] A204、处理装置对该需要加固的代码的索引进行加密，得到加密索引。

[0058] 例如，具体可以隐藏该索引，比如将该索引中的一些项目的值改写为无效值，等等。

[0059] A205、处理装置将加密索引添加至该可执行文件，比如dex文件中的相应位置，得到加固后的可执行文件。

[0060] (2)运行；

[0061] 如图2b所示，该加固后可执行文件的运行方法的具体流程可以如下：

[0062] B201、在启动移动终端应用时，处理装置启动本移动终端的微型虚拟机。

[0063] 例如，以安卓系统为例，具体可以利用安卓系统原有dalvik(一种用于Android平台的Java虚拟机)的解释运行的特性，来指定本移动终端专属的微型虚拟机，使得该微型虚拟机可以具有加固后的可执行文件运行前的最高优先运行权，即在加固后的可执行文件运行前优先运行微型虚拟机，这样，在启动移动终端应用时，便可以启动微型虚拟机。

[0064] B202、处理装置利用该微型虚拟机对微型虚拟机自身的完整性进行检测，若完整性检测通过，则执行步骤B203，若完整性检测不通过，则终止运行，流程结束。

[0065] B203、处理装置利用该微型虚拟机对可执行文件如dex文件的运行环境的安全性进行检测，若运行环境为安全，则执行步骤B204，若运行环境为不安全，则终止运行，流程结束。

[0066] B204、在完整性检测通过且运行环境为安全，处理装置将加固后的可执行文件加载至该微型虚拟机中，比如将加固后的dex文件加载至该微型虚拟机中。

[0067] B205、处理装置确定该加固后的可执行文件中加密索引的位置，根据确定的位置获取相应的加密索引。

[0068] B206、处理装置在该微型虚拟机中对加密索引进行解密，得到解密后代索引。

[0069] 其中，解密的方法与加密的方法想匹配，例如，如果在加密时隐藏了需要加固的代码的索引，则此时可以将隐藏的索引还原，比如，将一些项目的无效值还原为原有的值，等等。

[0070] B207、处理装置在该微型虚拟机中根据解密后索引还原该可执行文件如dex文件的代码，并在该微型虚拟机中运行还原后代码。

[0071] 由上可知，本实施例采用在启动移动终端应用时，启动微型虚拟机，利用该微型虚拟机对微信虚拟机自身的完整性，以及可执行文件运行环境的安全性进行检测，并在确定检测通过时，将加固后的可执行文件加载至该微型虚拟机中进行解密并运行；由于本方案在进行解密和运行代码之前，均会对运行环境进行检测，以保证运行环境的安全性，因此，可以更好地保护代码，提高数据安全性；而且，由于代码的解密和运行是在指定的微型虚拟机中进行的，因此，相对于现有技术只能在内存中进行解密和运行的方案而言，可以避免受

其他进程的影响，提高其运行效率，且兼容性更优。

[0072] 实施例三、

[0073] 为了更好地实施以上方法，本发明实施例还提供一种可执行文件的处理装置，如图3a所示，该可执行文件的处理装置可以包括启动单元301、检测单元302和处理单元303，如下：

[0074] 启动单元301，用于在启动移动终端应用时，启动微型虚拟机。

[0075] 例如，以安卓系统为例，具体可以利用安卓系统原有dalvik的解释运行的特性，来指定本移动终端专属的微型虚拟机，使得该微型虚拟机可以具有加固后的可执行文件运行前的最高优先运行权，即在加固后的可执行文件运行前优先运行微型虚拟机，这样，在启动移动终端应用时，便可以启动微型虚拟机。

[0076] 检测单元302，用于利用该微型虚拟机对可执行文件的运行环境进行检测。

[0077] 其中，对该运行环境的检测包括对微型虚拟机自身的完整性的检测，以及对运行环境的安全性的检测，即：

[0078] 检测单元302，具体用于利用该微型虚拟机对微型虚拟机自身的完整性进行检测；以及，利用该微型虚拟机对可执行文件的运行环境的安全性进行检测；若完整性检测通过且运行环境为安全，则确定检测结果符合预置条件；若完整性检测不通过或运行环境不安全，则确定检测结果不符合预置条件。

[0079] 其中，完整性检测和安全性检测的执行可以不分先后，在此不再赘述。

[0080] 处理单元303，用于确定检测结果符合预置条件时，将加固后的可执行文件加载至该微型虚拟机中进行解密并运行。

[0081] 例如，该处理单元303，具体可以用于将加固后的可执行文件加载至该微型虚拟机中，并确定该加固后的可执行文件中加密索引的位置；根据确定的位置获取相应的加密索引，并在该微型虚拟机中对加密索引进行解密，得到解密后索引；在该微型虚拟机中，根据解密后索引还原该可执行文件的代码并运行还原后代码。

[0082] 其中，加固后的可执行文件指的是加密后的可执行文件，加固的方式可以有多种，例如，可以获取可执行文件中需要加固的代码的索引，然后对该索引进行加密，即如图3b所示，该可执行文件的处理装置还可以包括获取单元304、加密单元305和添加单元306，如下：

[0083] 获取单元304，用于获取可执行文件中需要加固的代码的索引。

[0084] 例如，获取单元304，具体可以用于获取移动终端应用提交的关于可执行文件的加固请求，根据该加固请求扫描该移动终端应用的可执行文件，以获取需要加固的代码，然后根据预置的虚拟机特性获取该需要加固的代码的索引。

[0085] 加密单元305，用于对该需要加固的代码的索引进行加密，得到加密索引。

[0086] 其中，加密的方式可以有多种，具体可以根据实际应用的需求进行设置，在此不再赘述。

[0087] 添加单元306，用于将加密索引添加至该可执行文件中的相应位置，得到加固后的可执行文件。

[0088] 具体实施时，以上各个单元可以作为独立的实体来实现，也可以进行任意组合，作为同一或若干个实体来实现，以上各个单元的具体实施可参见前面的方法实施例，在此不再赘述。

[0089] 该可执行文件的处理装置具体可以集成在移动终端等设备中，该移动终端具体可以为手机或平板电脑等。

[0090] 由上可知，本实施例的可执行文件的处理装置的启动单元301可以在启动移动终端应用时，启动微型虚拟机，然后由检测单元302利用该微型虚拟机对可执行文件的运行环境进行检测，并在确定检测结果符合预置条件时，由处理单元303将加固后的可执行文件加载至该微型虚拟机中进行解密并运行；由于本方案在进行解密和运行代码之前，均会对运行环境进行检测，以保证运行环境的安全性，因此，可以更好地保护代码，提高数据安全性；而且，由于代码的解密和运行是在指定的微型虚拟机中进行的，因此，相对于现有技术只能在内存中进行解密和运行的方案而言，可以避免受其他进程的影响，提高其运行效率，且兼容性更优。

[0091] 实施例四、

[0092] 相应的，本发明实施例还提供一种可执行文件的处理系统，包括微型虚拟机和本发明实施例所提供的任一种可执行文件的处理装置，其中，该可执行文件的处理装置具体可参见实施例三，例如，具体可以如下：

[0093] 可执行文件的处理装置，用于在启动移动终端应用时，启动微型虚拟机；利用该微型虚拟机对可执行文件的运行环境进行检测；确定检测结果符合预置条件时，将加固后的可执行文件加载至该微型虚拟机中进行解密并运行。

[0094] 微型虚拟机，用于在该可执行文件的处理装置的控制下启动，并在该可执行文件的处理装置的控制下，对加载在本微型虚拟机中的加固后的可执行文件进行解密并运行。

[0095] 其中，加固后的可执行文件指的是加密后的可执行文件，加固的方式可以有多种，例如，具体可以如下：

[0096] 可执行文件的处理装置，还可以用于获取可执行文件中需要加固的代码的索引，对该需要加固的代码的索引进行加密，得到加密索引，将加密索引添加至该可执行文件中的相应位置，得到加固后的可执行文件。

[0097] 以上各个设备的具体实施可参见前面的实施例，在此不再赘述。

[0098] 由于该可执行文件的处理系统可以包括本发明实施例所提供的任一种可执行文件的处理装置，因此，可以实现本发明实施例所提供的任一种可执行文件的处理装置所能实现的有益效果，详见前面的实施例，在此不再赘述。

[0099] 实施例五、

[0100] 相应的，本发明实施例还提供一种移动终端，如图4所示，该移动终端可以包括射频(RF，Radio Frequency)电路401、包括有一个或一个以上计算机可读存储介质的存储器402、输入单元403、显示单元404、传感器405、音频电路406、无线保真(WiFi，Wireless Fidelity)模块407、包括有一个或者一个以上处理核心的处理器408、以及电源409等部件。本领域技术人员可以理解，图4中示出的移动终端结构并不构成对移动终端的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。其中：

[0101] RF电路401可用于收发信息或通话过程中，信号的接收和发送，特别地，将基站的下行信息接收后，交由一个或者一个以上处理器408处理；另外，将涉及上行的数据发送给基站。通常，RF电路401包括但不限于天线、至少一个放大器、调谐器、一个或多个振荡器、用户身份模块(SIM，Subscriber Identity Module)卡、收发信机、耦合器、低噪声放大器

(LNA,Low Noise Amplifier)、双工器等。此外,RF电路401还可以通过无线通信与网络和其他设备通信。所述无线通信可以使用任一通信标准或协议,包括但不限于全球移动通讯系统(GSM,Global System of Mobile communication)、通用分组无线服务(GPRS,General Packet Radio Service)、码分多址(CDMA,Code Division Multiple Access)、宽带码分多址(WCDMA,Wideband Code Division Multiple Access)、长期演进(LTE,Long Term Evolution)、电子邮件、短消息服务(SMS,Short Messaging Service)等。

[0102] 存储器402可用于存储软件程序以及模块,处理器408通过运行存储在存储器402的软件程序以及模块,从而执行各种功能应用以及数据处理。存储器402可主要包括存储程序区和存储数据区,其中,存储程序区可存储操作系统、至少一个功能所需的应用程序(比如声音播放功能、图像播放功能等)等;存储数据区可存储根据移动终端的使用所创建的数据(比如音频数据、电话本等)等。此外,存储器402可以包括高速随机存取存储器,还可以包括非易失性存储器,例如至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。相应地,存储器402还可以包括存储器控制器,以提供处理器408和输入单元403对存储器402的访问。

[0103] 输入单元403可用于接收输入的数字或字符信息,以及产生与用户设置以及功能控制有关的键盘、鼠标、操作杆、光学或者轨迹球信号输入。具体地,在一个具体的实施例中,输入单元403可包括触敏表面以及其他输入设备。触敏表面,也称为触摸显示屏或者触控板,可收集用户在其上或附近的触摸操作(比如用户使用手指、触笔等任何适合的物体或附件在触敏表面上或在触敏表面附近的操作),并根据预先设定的程式驱动相应的连接装置。可选的,触敏表面可包括触摸检测装置和触摸控制器两个部分。其中,触摸检测装置检测用户的触摸方位,并检测触摸操作带来的信号,将信号传送给触摸控制器;触摸控制器从触摸检测装置上接收触摸信息,并将它转换成触点坐标,再送给处理器408,并能接收处理器408发来的命令并加以执行。此外,可以采用电阻式、电容式、红外线以及表面声波等多种类型实现触敏表面。除了触敏表面,输入单元403还可以包括其他输入设备。具体地,其他输入设备可以包括但不限于物理键盘、功能键(比如音量控制按键、开关按键等)、轨迹球、鼠标、操作杆等中的一种或多种。

[0104] 显示单元404可用于显示由用户输入的信息或提供给用户的信息以及移动终端的各种图形用户接口,这些图形用户接口可以由图形、文本、图标、视频和其任意组合来构成。显示单元404可包括显示面板,可选的,可以采用液晶显示器(LCD,Liquid Crystal Display)、有机发光二极管(OLED,Organic Light-Emitting Diode)等形式来配置显示面板。进一步的,触敏表面可覆盖显示面板,当触敏表面检测到在其上或附近的触摸操作后,传送给处理器408以确定触摸事件的类型,随后处理器408根据触摸事件的类型在显示面板上提供相应的视觉输出。虽然在图4中,触敏表面与显示面板是作为两个独立的部件来实现输入和输入功能,但是在某些实施例中,可以将触敏表面与显示面板集成而实现输入和输出功能。

[0105] 移动终端还可包括至少一种传感器405,比如光传感器、运动传感器以及其他传感器。具体地,光传感器可包括环境光传感器及接近传感器,其中,环境光传感器可根据环境光线的明暗来调节显示面板的亮度,接近传感器可在移动终端移动到耳边时,关闭显示面板和/或背光。作为运动传感器的一种,重力加速度传感器可检测各个方向上(一般为三轴)

加速度的大小，静止时可检测出重力的大小及方向，可用于识别手机姿态的应用(比如横竖屏切换、相关游戏、磁力计姿态校准)、振动识别相关功能(比如计步器、敲击)等；至于移动终端还可配置的陀螺仪、气压计、湿度计、温度计、红外线传感器等其他传感器，在此不再赘述。

[0106] 音频电路406、扬声器，传声器可提供用户与移动终端之间的音频接口。音频电路406可将接收到的音频数据转换后的电信号，传输到扬声器，由扬声器转换为声音信号输出；另一方面，传声器将收集的声音信号转换为电信号，由音频电路406接收后转换为音频数据，再将音频数据输出处理器408处理后，经RF电路401以发送给比如另一移动终端，或者将音频数据输出至存储器402以便进一步处理。音频电路406还可能包括耳塞插孔，以提供外设耳机与移动终端的通信。

[0107] WiFi属于短距离无线传输技术，移动终端通过WiFi模块407可以帮助用户收发电子邮件、浏览网页和访问流式媒体等，它为用户提供了无线的宽带互联网访问。虽然图4示出了WiFi模块407，但是可以理解的是，其并不属于移动终端的必须构成，完全可以根据需要在不改变发明的本质的范围内而省略。

[0108] 处理器408是移动终端的控制中心，利用各种接口和线路连接整个手机的各个部分，通过运行或执行存储在存储器402内的软件程序和/或模块，以及调用存储在存储器402内的数据，执行移动终端的各种功能和处理数据，从而对手机进行整体监控。可选的，处理器408可包括一个或多个处理核心；优选的，处理器408可集成应用处理器和调制解调处理器，其中，应用处理器主要处理操作系统、用户界面和应用程序等，调制解调处理器主要处理无线通信。可以理解的是，上述调制解调处理器也可以不集成到处理器408中。

[0109] 移动终端还包括给各个部件供电的电源409(比如电池)，优选的，电源可以通过电源管理系统与处理器408逻辑相连，从而通过电源管理系统实现管理充电、放电、以及功耗管理等功能。电源409还可以包括一个或一个以上的直流或交流电源、再充电系统、电源故障检测电路、电源转换器或者逆变器、电源状态指示器等任意组件。

[0110] 尽管未示出，移动终端还可以包括摄像头、蓝牙模块等，在此不再赘述。具体在本实施例中，移动终端中的处理器408会按照如下的指令，将一个或一个以上的应用程序的进程对应的可执行文件加载到存储器402中，并由处理器408来运行存储在存储器402中的应用程序，从而实现各种功能：

[0111] 在启动移动终端应用时，启动微型虚拟机；利用该微型虚拟机对可执行文件的运行环境进行检测；确定检测结果符合预置条件时，将加固后的可执行文件加载至该微型虚拟机中进行解密并运行。

[0112] 其中，对该运行环境的检测包括对微型虚拟机自身的完整性的检测，以及对运行环境的安全性的检测，具体可参见前面的实施例。

[0113] 此外，需说明的是，加固后的可执行文件指的是加密后的可执行文件，其中，加固的方式可以有多种，例如，具体可以如下：

[0114] 获取可执行文件中需要加固的代码的索引，对该需要加固的代码的索引进行加密，得到加密索引，将加密索引添加至该可执行文件中的相应位置，得到加固后的可执行文件，详见前面的实施例。

[0115] 以上各个操作的具体实施可参见前面的实施例，在此不再赘述。

[0116] 由上可知，本实施例的移动终端采用在启动移动终端应用时，启动微型虚拟机，利用该微型虚拟机对可执行文件的运行环境进行检测，并在确定检测结果符合预置条件时，将加固后的可执行文件加载至该微型虚拟机中进行解密并运行；由于本方案在进行解密和运行代码之前，均会对运行环境进行检测，以保证运行环境的安全性，因此，可以更好地保护代码，提高数据安全性；而且，由于代码的解密和运行是在指定的微型虚拟机中进行的，因此，相对于现有技术只能在内存中进行解密和运行的方案而言，可以避免受其他进程的影响，提高其运行效率，且兼容性更优。

[0117] 本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括：只读存储器(ROM，Read Only Memory)、随机存取记忆体(RAM，Random Access Memory)、磁盘或光盘等。

[0118] 以上对本发明实施例所提供的一种可执行文件的处理方法、装置和系统进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

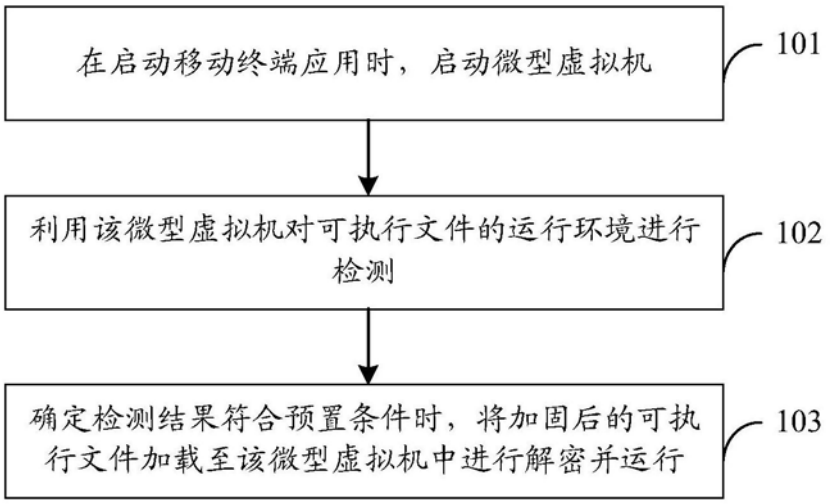

在启动移动终端应用时，启动微型虚拟机
101
利用该微型虚拟机对可执行文件的运行环境进行检测
102
确定检测结果符合预置条件时，将加固后的可执行文件加载至该微型虚拟机中进行解密并运行
103

图1

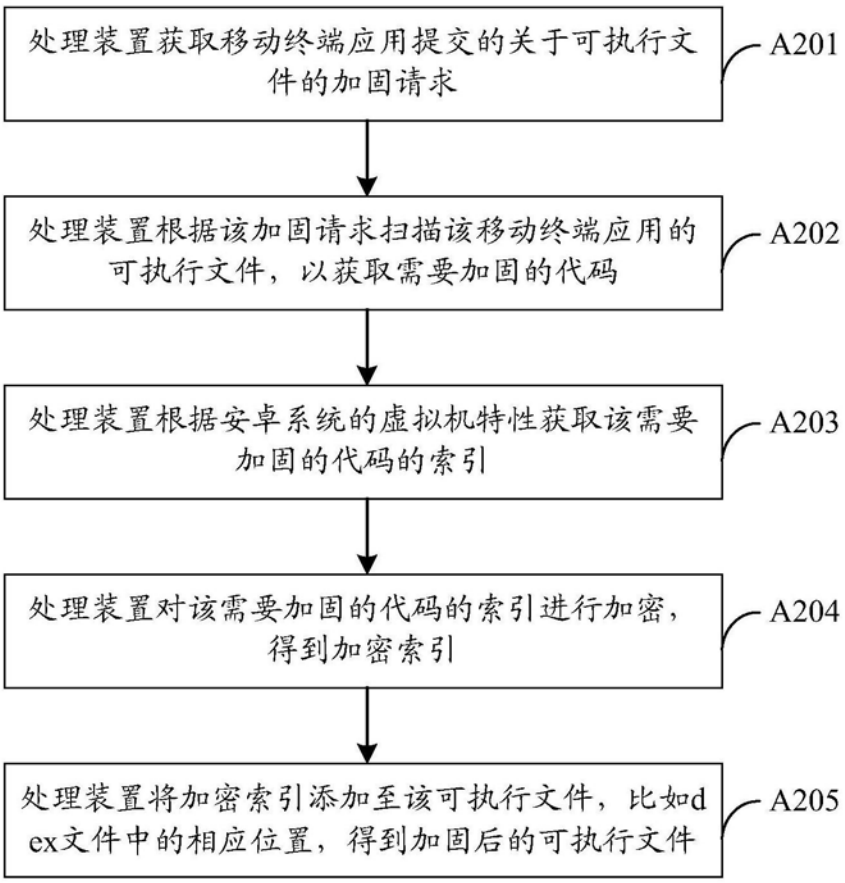

处理装置获取移动终端应用提交的关于可执行文件的加固请求
A201
处理装置根据该加固请求扫描该移动终端应用的可执行文件，以获取需要加固的代码
A202
处理装置根据安卓系统的虚拟机特性获取该需要加固的代码的索引
A203
处理装置对该需要加固的代码的索引进行加密，得到加密索引
A204
处理装置将加密索引添加至该可执行文件，比如dex文件中的相应位置，得到加固后的可执行文件
A205

图2a

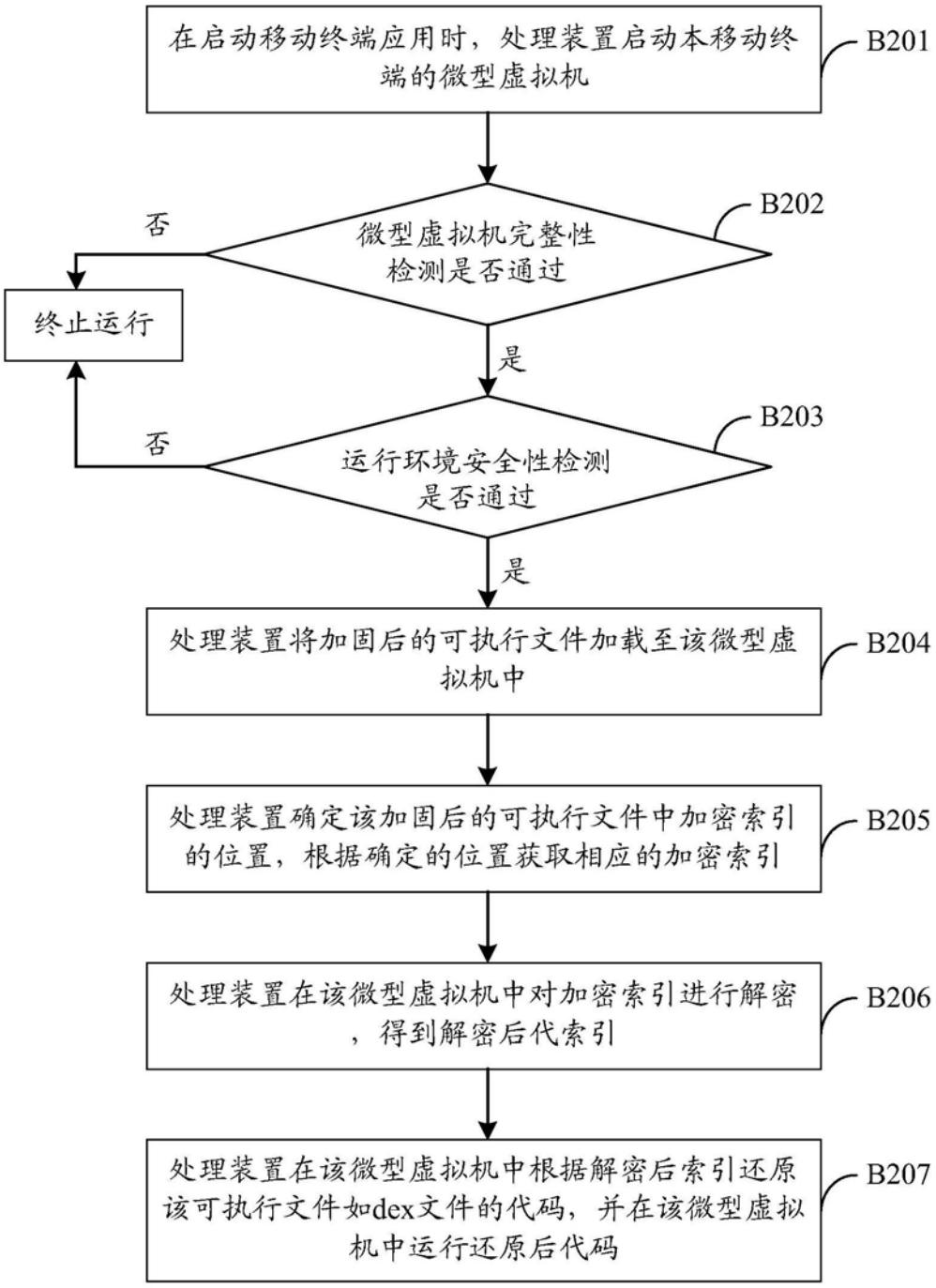

在启动移动终端应用时，处理装置启动本移动终端的微型虚拟机
B201
微型虚拟机完整性检测是否通过
B202
否
终止运行
是
运行环境安全性检测是否通过
B203
否
是
处理装置将加固后的可执行文件加载至该微型虚拟机中
B204
处理装置确定该加固后的可执行文件中加密索引的位置，根据确定的位置获取相应的加密索引
B205
处理装置在该微型虚拟机中对加密索引进行解密，得到解密后代索引
B206
处理装置在该微型虚拟机中根据解密后索引还原该可执行文件如dex文件的代码，并在该微型虚拟机中运行还原后代码
B207

图2b

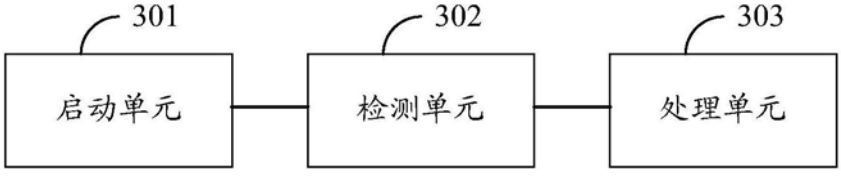

301
启动单元
302
检测单元
303
处理单元

图3a

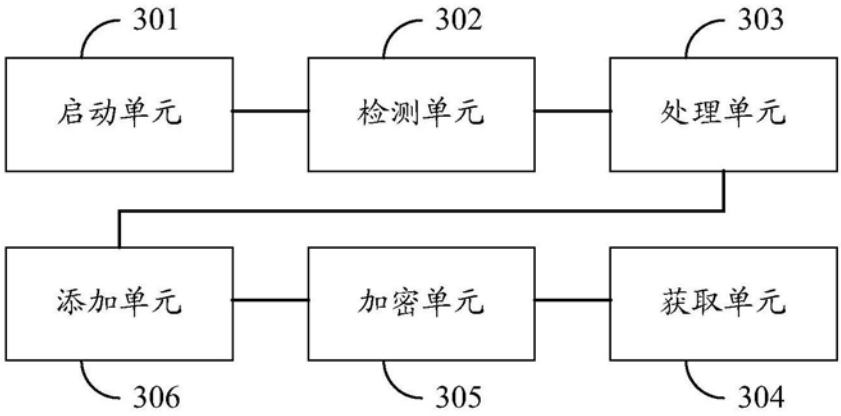

301
302
303
启动单元
检测单元
处理单元
添加单元
加密单元
获取单元
306
305
304

图3b

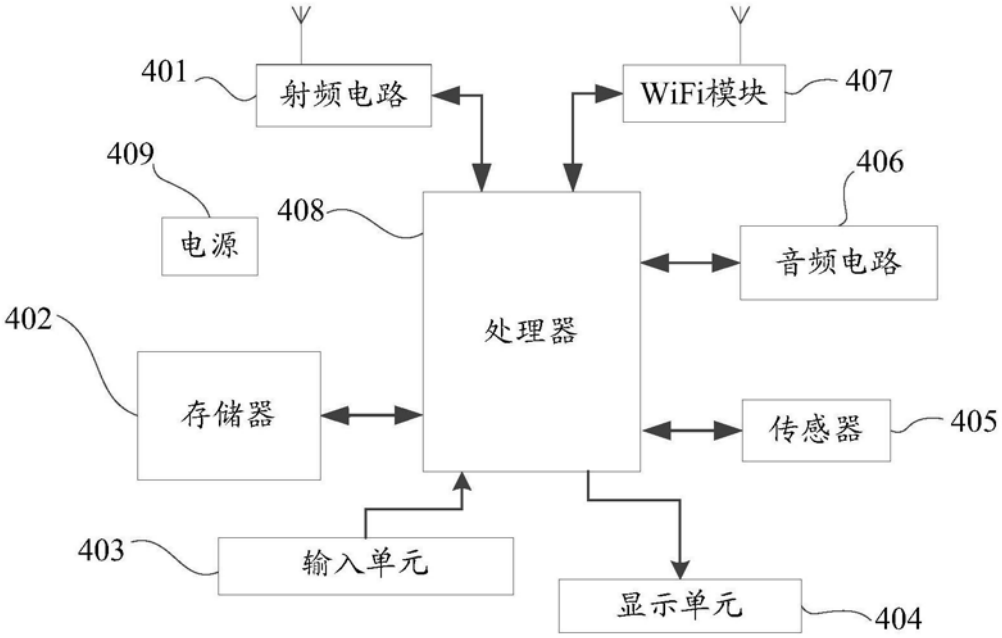

401
射频电路
WiFi模块
407
409
电源
408
处理器
406
音频电路
402
存储器
传感器
405
403
输入单元
显示单元
404

图4