(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 106295257 A
(43)申请公布日 2017.01.04

(21)申请号 201510366915.9

(22)申请日 2015.06.29

(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

(72)发明人 李晖 王蔚 董振江 张文 张亚腾

(74)专利代理机构 北京银龙知识产权代理有限公司 11243
代理人 许静 安利霞

(51)Int.Cl.
G06F 21/12(2013.01)
G06F 21/64(2013.01)

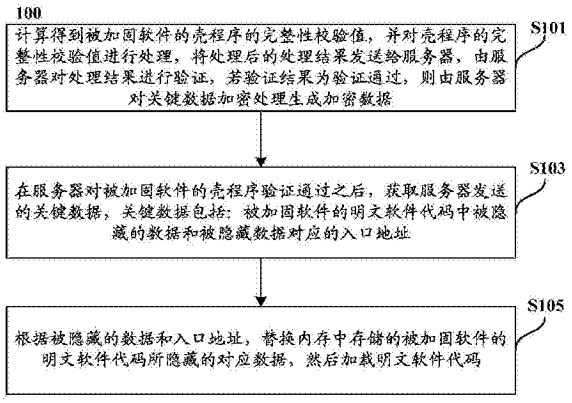
权利要求书4页 说明书10页 附图7页

(54)发明名称

一种被加固软件的认证方法及装置

(57)摘要

本发明提供了一种被加固软件的认证方法及装置，该认证方法包括：在服务器对被加固软件的壳程序验证通过之后，获取服务器发送的关键数据，关键数据包括：被加固软件的明文软件代码中被隐藏的数据和被隐藏数据对应的入口地址；根据被隐藏的数据和入口地址，替换内存中存储的被加固软件的明文软件代码所隐藏的对应数据，然后加载明文软件代码。通过本发明提供的认证方法既能够有效分清服务请求的来源，又能够在恶意应用请求提供服务时，进行有效的保护，大大提高了对被加固软件的保护强度，有效地防止攻击者的攻击，保证被加固软件可以正常运行。



CN 106295257 A

1. 一种被加固软件的认证方法，应用于一移动终端，其特征在于，所述认证方法包括：

在服务器对被加固软件的壳程序验证通过之后，获取所述服务器发送的关键数据，所述关键数据包括：所述被加固软件的明文软件代码中被隐藏的数据和所述被隐藏数据对应的入口地址；

根据所述被隐藏的数据和所述入口地址，替换内存中存储的所述被加固软件的明文软件代码所隐藏的对应数据，然后加载所述明文软件代码。

2. 如权利要求 1 所述的认证方法，其特征在于，在服务器对被加固软件的壳程序验证通过之前，所述认证方法还包括：

计算得到被加固软件的壳程序的完整性校验值，并对所述壳程序的完整性校验值进行处理，将处理后的处理结果发送给所述服务器，由所述服务器对所述处理结果进行验证，若验证结果为验证通过，则由所述服务器对关键数据加密处理生成加密数据。

3. 如权利要求 2 所述的认证方法，其特征在于，所述计算得到被加固软件的壳程序的完整性校验值，并对所述壳程序的完整性校验值进行处理，将处理后的处理结果发送给所述服务器，由所述服务器对所述处理结果进行验证，若验证结果为验证通过，则由所述服务器对关键数据加密处理生成加密数据，具体包括：

将所述被加固软件的请求信息发送给服务器，由所述服务器根据所述被加固软件的请求信息随机生成第一随机数；

根据第一算法计算得到被加固软件的壳程序的完整性校验值；

获取所述第一随机数，将所述第一随机数与所述壳程序的完整性校验值进行第一级联处理，获取第一级联结果；

根据第二算法对所述第一级联结果进行计算，获取第一计算结果；

将所述第一计算结果与所述被加固软件随机生成的第二随机数进行第二级联处理，并将处理结果发送给所述服务器，由所述服务器对所述处理结果进行验证，若验证结果为验证通过，则由所述服务器对关键数据加密处理生成加密数据。

4. 如权利要求 3 所述的认证方法，其特征在于，所述在服务器对被加固软件的壳程序验证通过之后，获取所述服务器发送的关键数据，具体包括：

在服务器对被加固软件的壳程序验证通过之后，对所述服务器发送的加密数据进行解密运算；

所述解密运算完成后，获取解密数据中包含的所述服务器发送的关键数据。

5. 如权利要求 1 所述的认证方法，其特征在于，所述根据所述被隐藏的数据和所述入口地址，替换内存中存储的所述被加固软件的明文软件代码所隐藏的对应数据，然后加载所述明文软件代码，具体包括：

根据所述入口地址，定位所述被加固软件的明文软件代码所隐藏的对应数据在所述被加固软件的明文软件代码中的位置；

将所述被隐藏的数据替换内存中存储的所述被加固软件的明文软件代码所隐藏的对应数据，然后加载所述明文软件代码。

6. 一种被加固软件的认证方法，应用于一服务器，其特征在于，所述认证方法包括：

获取被加固软件发送的处理结果，对所述被加固软件的壳程序的完整性校验值进行验证；

若所述验证结果为验证通过，则对关键数据进行加密处理，并将加密生成的加密数据发送给所述被加固软件，所述关键数据包括：所述被加固软件的明文软件代码中被隐藏的数据和所述被隐藏数据对应的入口地址。

7. 如权利要求 6 所述的认证方法，其特征在于，所述根据被加固软件发送的处理结果，对所述被加固软件的壳程序的完整性校验值进行验证，具体包括：

获取被加固软件的请求信息，根据所述请求信息随机生成第一随机数，并将所述第一随机数发送给所述被加固软件；

根据所述被加固软件的请求信息获取所述被加固软件的 ID 信息，并根据所述被加固软件的 ID 信息获取所述被加固软件的壳程序的完整性校验值，将所述第一随机数与所述壳程序的完整性校验值进行第一级联处理，获取第二级联结果；

根据第二算法对所述第二级联结果进行计算，得到第二计算结果；

获取所述被加固软件发送的处理结果，根据所述处理结果识别获取第一计算结果和第二随机数；

对所述第一计算结果与所述第二计算结果进行验证，若所述第一计算结果与所述第二计算结果相同，则验证结果为验证通过。

8. 如权利要求 7 所述的认证方法，其特征在于，所述若所述验证结果为验证通过，则对关键数据进行加密处理，将加密生成的加密数据发送给所述被加固软件，具体包括：

获取根据所述第二级联结果识别得到的所述第二随机数；

所述第二随机数与关键数据中包括的所述被隐藏数据对应的入口地址根据第三算法进行计算，并得到第三计算结果；

对所述第三计算结果进行加密处理，将加密后生成的加密数据发送给所述被加固软件。

9. 如权利要求 8 所述的认证方法，其特征在于，所述将所述第二随机数与所述被加固软件的明文软件代码中的入口地址根据第三算法进行计算，具体为：

对所述第二随机数与所述被加固软件的明文软件代码中的入口地址进行异或的逻辑运算。

10. 一种被加固软件的认证装置，应用于一移动终端，其特征在于，所述认证装置包括：

获取模块，用于在服务器对被加固软件的壳程序验证通过之后，获取所述服务器发送的关键数据，所述关键数据包括：所述被加固软件的明文软件代码中被隐藏的数据和所述被隐藏数据对应的入口地址；

替换模块，用于根据所述被隐藏的数据和所述入口地址，替换内存中存储的所述被加固软件的明文软件代码所隐藏的对应数据，然后加载所述明文软件代码。

11. 如权利要求 10 所述的认证装置，其特征在于，所述认证装置还包括：

处理模块，用于计算得到被加固软件的壳程序的完整性校验值，并对所述壳程序的完整性校验值进行处理，将处理后的处理结果发送给所述服务器，由所述服务器对所述处理结果进行验证，若验证结果为验证通过，则由所述服务器对关键数据加密处理生成加密数据。

12. 如权利要求 11 所述的认证装置，其特征在于，所述处理模块具体包括：

发送单元，用于将所述被加固软件的请求信息发送给服务器，由所述服务器根据所述被加固软件的请求信息随机生成第一随机数；

第一计算单元，用于根据第一算法计算得到被加固软件的壳程序的完整性校验值；

第一级联单元，用于获取所述第一随机数，将所述第一随机数与所述壳程序的完整性校验值进行第一级联处理，获取第一级联结果；

第二计算单元，用于根据第二算法对所述第一级联结果进行计算，获取第一计算结果；

第二级联单元，用于将所述第一计算结果与所述被加固软件随机生成的第二随机数进行第二级联处理，并将处理结果发送给所述服务器，由所述服务器对所述处理结果进行验证，若验证结果为验证通过，则由所述服务器对关键数据加密处理生成加密数据。

13. 如权利要求 12 所述的认证装置，其特征在于，所述获取模块具体包括：

解密单元，用于在服务器对被加固软件的壳程序验证通过之后，对所述服务器发送的加密数据进行解密运算；

第一获取单元，用于所述解密运算完成后，获取解密数据中包含的所述服务器发送的关键数据。

14. 如权利要求 10 所述的认证装置，其特征在于，所述替换模块具体包括：

定位单元，用于根据所述入口地址，定位所述被加固软件的明文软件代码所隐藏的对应数据在所述被加固软件的明文软件代码中的位置；

替换单元，用于将所述被隐藏的数据替换内存中存储的所述被加固软件的明文软件代码所隐藏的对应数据，然后加载所述明文软件代码。

15. 一种被加固软件的认证装置，应用于一服务器，其特征在于，所述认证装置包括：

验证模块，用于获取被加固软件发送的处理结果，对所述被加固软件的壳程序的完整性校验值进行验证；

加密模块，用于若所述验证结果为验证通过，则对关键数据进行加密处理，将加密生成的加密数据发送给所述被加固软件，所述关键数据包括：所述被加固软件的明文软件代码中被隐藏的数据和所述被隐藏数据对应的入口地址。

16. 如权利要求 15 所述的认证装置，其特征在于，所述验证模块具体包括：

生成单元，用于获取被加固软件的请求信息，根据所述请求信息随机生成第一随机数，并将所述第一随机数发送给所述被加固软件；

第三级联单元，用于根据所述被加固软件的请求信息获取所述被加固软件的 ID 信息，并根据所述被加固软件的 ID 信息获取所述被加固软件的壳程序的完整性校验值，将所述第一随机数与所述壳程序的完整性校验值进行第一级联处理，获取第二级联结果；

第三计算单元，用于根据第二算法对所述第二级联结果进行计算，得到第二计算结果；

识别单元，用于获取所述被加固软件发送的处理结果，根据所述处理结果识别获取第一计算结果和第二随机数；

验证单元，用于对所述第一计算结果与所述第二计算结果进行验证，若所述第一计算结果与所述第二计算结果相同，则验证结果为验证通过。

17. 如权利要求 16 所述的认证装置，其特征在于，所述添加模块具体包括：

第二获取单元，用于获取根据所述第二级联结果识别得到的所述第二随机数；

第四计算单元，用于所述第二随机数与关键数据中包括的所述被隐藏数据对应的入口地址根据第三算法进行计算，并得到第三计算结果；

加密单元，用于对所述第三计算结果进行加密处理，将加密后生成的加密数据发送给所述被加固软件。

18. 如权利要求 17 所述的认证装置，其特征在于，所述第四计算单元在根据所述第三算法进行计算时，具体为：

对所述第二随机数与所述被加固软件的明文软件代码中的入口地址进行异或的逻辑运算。

一种被加固软件的认证方法及装置

技术领域

[0001] 本发明涉及互联网安全技术领域，尤其涉及一种被加固软件的认证方法及装置。

背景技术

[0002] 在安卓(Android)系统中，为了安全的需要，我们会对应用软件安装包做相应的加固处理，并且相应的希望市场上流通的都是经过加固处理的安装包。但是现有的安卓软件市场种类繁多，对同一软件安装包的发布也会有很多自定义的版本。

[0003] 对安卓系统的服务而言，当作为应用的服务运行时，会启动一个新的进程或者利用应用现有进程，创建一个服务对象。当其他应用调用到此服务时由此服务对象的代码完成具体的业务逻辑。

[0004] 然而按照现有安卓系统的服务提供方式，服务提供应用无法对提供的数据进行存取保护。即使服务请求应用在存取数据时进行安全提示，但对用户而言，也不能有效分清服务请求的来源，在恶意应用请求提供服务时，无法进行有效的保护。为避免未经保护的安装包在市面上的安装传播，需要对应用软件进行认证。

发明内容

[0005] 为了克服上述问题，本发明提供了一种被加固软件的认证方法及装置，既能够有效分清服务请求的来源，又能够在恶意应用请求提供服务时，进行有效的保护，大大提高了对被加固软件的保护强度，有效地防止攻击者的攻击，保证被加固软件可以正常运行。

[0006] 为了解决上述技术问题，本发明采用如下技术方案：

[0007] 依据本发明的一个方面，提供了一种被加固软件的认证方法，应用于一移动终端，所述认证方法包括：

[0008] 在服务器对被加固软件的壳程序验证通过之后，获取所述服务器发送的关键数据，所述关键数据包括：所述被加固软件的明文软件代码中被隐藏的数据和所述被隐藏数据对应的入口地址；

[0009] 根据所述被隐藏的数据和所述入口地址，替换内存中存储的所述被加固软件的明文软件代码所隐藏的对应数据，然后加载所述明文软件代码。

[0010] 可选地，在服务器对被加固软件的壳程序验证通过之前，所述认证方法还包括：

[0011] 计算得到被加固软件的壳程序的完整性校验值，并对所述壳程序的完整性校验值进行处理，将处理后的处理结果发送给所述服务器，由所述服务器对所述处理结果进行验证，若验证结果为验证通过，则由所述服务器对关键数据加密处理生成加密数据。

[0012] 可选地，所述计算得到被加固软件的壳程序的完整性校验值，并对所述壳程序的完整性校验值进行处理，将处理后的处理结果发送给所述服务器，由所述服务器对所述处理结果进行验证，若验证结果为验证通过，则由所述服务器对关键数据加密处理生成加密数据，具体包括：

[0013] 将所述被加固软件的请求信息发送给服务器，由所述服务器根据所述被加固软件

的请求信息随机生成第一随机数；

[0014] 根据第一算法计算得到被加固软件的壳程序的完整性校验值；

[0015] 获取所述第一随机数，将所述第一随机数与所述壳程序的完整性校验值进行第一级联处理，获取第一级联结果；

[0016] 根据第二算法对所述第一级联结果进行计算，获取第一计算结果；

[0017] 将所述第一计算结果与所述被加固软件随机生成的第二随机数进行第二级联处理，并将处理结果发送给所述服务器，由所述服务器对所述处理结果进行验证，若验证结果为验证通过，则由所述服务器对关键数据加密处理生成加密数据。

[0018] 可选地，所述在服务器对被加固软件的壳程序验证通过之后，获取所述服务器发送的关键数据，具体包括：

[0019] 在服务器对被加固软件的壳程序验证通过之后，对所述服务器发送的加密数据进行解密运算；

[0020] 所述解密运算完成后，获取解密数据中包含的所述服务器发送的关键数据。

[0021] 可选地，所述根据所述被隐藏的数据和所述入口地址，替换内存中存储的所述被加固软件的明文软件代码所隐藏的对应数据，然后加载所述明文软件代码，具体包括：

[0022] 根据所述入口地址，定位所述被加固软件的明文软件代码所隐藏的对应数据在所述被加固软件的明文软件代码中的位置；

[0023] 将所述被隐藏的数据替换内存中存储的所述被加固软件的明文软件代码所隐藏的对应数据，然后加载所述明文软件代码。

[0024] 依据本发明的另一方面，还提供了一种被加固软件的认证方法，应用于一服务器，所述认证方法包括：

[0025] 获取被加固软件发送的处理结果，对所述被加固软件的壳程序的完整性校验值进行验证；

[0026] 若所述验证结果为验证通过，则对关键数据进行加密处理，并将加密生成的加密数据发送给所述被加固软件，所述关键数据包括：所述被加固软件的明文软件代码中被隐藏的数据和所述被隐藏数据对应的入口地址。

[0027] 可选地，所述根据被加固软件发送的处理结果，对所述被加固软件的壳程序的完整性校验值进行验证，具体包括：

[0028] 获取被加固软件的请求信息，根据所述请求信息随机生成第一随机数，并将所述第一随机数发送给所述被加固软件；

[0029] 根据所述被加固软件的请求信息获取所述被加固软件的 ID 信息，并根据所述被加固软件的 ID 信息获取所述被加固软件的壳程序的完整性校验值，将所述第一随机数与所述壳程序的完整性校验值进行第一级联处理，获取第二级联结果；

[0030] 根据第二算法对所述第二级联结果进行计算，得到第二计算结果；

[0031] 获取所述被加固软件发送的处理结果，根据所述处理结果识别获取第一计算结果和第二随机数；

[0032] 对所述第一计算结果与所述第二计算结果进行验证，若所述第一计算结果与所述第二计算结果相同，则验证结果为验证通过。

[0033] 可选地，所述若所述验证结果为验证通过，则对关键数据进行加密处理，将加密生

成的加密数据发送给所述被加固软件，具体包括：

[0034] 获取根据所述第二级联结果识别得到的所述第二随机数；

[0035] 所述第二随机数与关键数据中包括的所述被隐藏数据对应的入口地址根据第三算法进行计算，并得到第三计算结果；

[0036] 对所述第三计算结果进行加密处理，将加密后生成的加密数据发送给所述被加固软件。

[0037] 可选地，所述将所述第二随机数与所述被加固软件的明文软件代码中的入口地址根据第三算法进行计算，具体为：

[0038] 对所述第二随机数与所述被加固软件的明文软件代码中的入口地址进行异或的逻辑运算。

[0039] 依据本发明的另一个方面，还提供了一种被加固软件的认证装置，应用于一移动终端，所述认证装置包括：

[0040] 获取模块，用于在服务器对被加固软件的壳程序验证通过之后，获取所述服务器发送的关键数据，所述关键数据包括：所述被加固软件的明文软件代码中被隐藏的数据和所述被隐藏数据对应的入口地址；

[0041] 替换模块，用于根据所述被隐藏的数据和所述入口地址，替换内存中存储的所述被加固软件的明文软件代码所隐藏的对应数据，然后加载所述明文软件代码。

[0042] 可选地，所述认证装置还包括：

[0043] 处理模块，用于计算得到被加固软件的壳程序的完整性校验值，并对所述壳程序的完整性校验值进行处理，将处理后的处理结果发送给所述服务器，由所述服务器对所述处理结果进行验证，若验证结果为验证通过，则由所述服务器对关键数据加密处理生成加密数据。

[0044] 可选地，所述处理模块具体包括：

[0045] 发送单元，用于将所述被加固软件的请求信息发送给服务器，由所述服务器根据所述被加固软件的请求信息随机生成第一随机数；

[0046] 第一计算单元，用于根据第一算法计算得到被加固软件的壳程序的完整性校验值；

[0047] 第一级联单元，用于获取所述第一随机数，将所述第一随机数与所述壳程序的完整性校验值进行第一级联处理，获取第一级联结果；

[0048] 第二计算单元，用于根据第二算法对所述第一级联结果进行计算，获取第一计算结果；

[0049] 第二级联单元，用于将所述第一计算结果与所述被加固软件随机生成的第二随机数进行第二级联处理，并将处理结果发送给所述服务器，由所述服务器对所述处理结果进行验证，若验证结果为验证通过，则由所述服务器对关键数据加密处理生成加密数据。

[0050] 可选地，所述获取模块具体包括：

[0051] 解密单元，用于在服务器对被加固软件的壳程序验证通过之后，对所述服务器发送的加密数据进行解密运算；

[0052] 第一获取单元，用于所述解密运算完成后，获取解密数据中包含的所述服务器发送的关键数据。

[0053] 可选地，所述替换模块具体包括：

[0054] 定位单元，用于根据所述入口地址，定位所述被加固软件的明文软件代码所隐藏的对应数据在所述被加固软件的明文软件代码中的位置；

[0055] 替换单元，用于将所述被隐藏的数据替换内存中存储的所述被加固软件的明文软件代码所隐藏的对应数据，然后加载所述明文软件代码。

[0056] 依据本发明的另一方面，还提供了一种被加固软件的认证装置，应用于一服务器，所述认证装置包括：

[0057] 验证模块，用于获取被加固软件发送的处理结果，对所述被加固软件的壳程序的完整性校验值进行验证；

[0058] 加密模块，用于若所述验证结果为验证通过，则对关键数据进行加密处理，将加密生成的加密数据发送给所述被加固软件，所述关键数据包括：所述被加固软件的明文软件代码中被隐藏的数据和所述被隐藏数据对应的入口地址。

[0059] 可选地，所述验证模块具体包括：

[0060] 生成单元，用于获取被加固软件的请求信息，根据所述请求信息随机生成第一随机数，并将所述第一随机数发送给所述被加固软件；

[0061] 第三级联单元，用于根据所述被加固软件的请求信息获取所述被加固软件的ID信息，并根据所述被加固软件的ID信息获取所述被加固软件的壳程序的完整性校验值，将所述第一随机数与所述壳程序的完整性校验值进行第一级联处理，获取第二级联结果；

[0062] 第三计算单元，用于根据第二算法对所述第二级联结果进行计算，得到第二计算结果；

[0063] 识别单元，用于获取所述被加固软件发送的处理结果，根据所述处理结果识别获取第一计算结果和第二随机数；

[0064] 验证单元，用于对所述第一计算结果与所述第二计算结果进行验证，若所述第一计算结果与所述第二计算结果相同，则验证结果为验证通过。

[0065] 可选地，所述添加模块具体包括：

[0066] 第二获取单元，用于获取根据所述第二级联结果识别得到的所述第二随机数；

[0067] 第四计算单元，用于所述第二随机数与关键数据中包括的所述被隐藏数据对应的入口地址根据第三算法进行计算，并得到第三计算结果；

[0068] 加密单元，用于对所述第三计算结果进行加密处理，将加密后生成的加密数据发送给所述被加固软件。

[0069] 可选地，所述第四计算单元在根据所述第三算法进行计算时，具体为：

[0070] 对所述第二随机数与所述被加固软件的明文软件代码中的入口地址进行异或的逻辑运算。

[0071] 本发明的有益效果是：

[0072] 本发明中提供的被加固软件的认证方法，在服务器对被加固软件的壳程序验证通过之后，可获取服务器提供的关键数据，并根据关键数据中的被加固软件的明文软件代码中被隐藏的数据对应的入口地址，能够确定内存中存储的被加固软件的明文软件代码所隐藏的对应数据在明文软件代码中的位置，然后用关键数据中包括的明文软件代码中被隐藏的数据替换内存中存储的被加固软件的明文软件代码所隐藏的对应数据，保证了该被加固

软件正常运行。另外，通过对被加固软件的壳程序进行验证，有效地防止壳程序被篡改，保证了壳程序的完整性。所以，通过本发明提供的认证方法既能够有效分清服务请求的来源，又能够在恶意应用请求提供服务时，进行有效的保护，大大提高了对被加固软件的保护强度，有效地防止攻击者的攻击，保证被加固软件可以正常运行。

附图说明

[0073] 图 1 表示本发明实施例中被加固软件的认证方法的流程图之一；

[0074] 图 2 表示本发明实施例中对壳程序的完整性校验值进行处理的流程图；

[0075] 图 3 表示本发明实施例中获取关键数据的流程图；

[0076] 图 4 表示本发明实施例中替换明文软件代码所隐藏的对应数据的流程图；

[0077] 图 5 表示本发明实施例中被加固软件的认证方法的流程图之二；

[0078] 图 6 表示本发明实施例中验证壳程序的完整性校验值的流程图；

[0079] 图 7 表示本发明实施例中加密关键数据的流程图；

[0080] 图 8 表示本发明实施例中被加固软件的认证装置的结构框图之一；

[0081] 图 9 表示本发明实施例中处理模块的结构框图；

[0082] 图 10 表示本发明实施例中获取模块的结构框图；

[0083] 图 11 表示本发明实施例中替换模块的结构框图；

[0084] 图 12 表示本发明实施例中被加固软件的认证装置的结构框图之二；

[0085] 图 13 表示本发明实施例中验证模块的结构框图；以及

[0086] 图 14 表示本发明实施例中加密模块的结构框图。

具体实施方式

[0087] 为使本发明的目的、技术方案和优点更加清楚，下面将结合附图及具体实施例对本发明进行详细描述。

[0088] 实施例一

[0089] 依据本发明的一个方面，提供了一种被加固软件的认证方法，应用于一移动终端，如图 1 所示，该认证方法 100 包括：

[0090] 步骤 S103、在服务器对被加固软件的壳程序验证通过之后，获取服务器发送的关键数据，关键数据包括：被加固软件的明文软件代码中被隐藏的数据和被隐藏数据对应的入口地址；

[0091] 步骤 S105、根据被隐藏的数据和入口地址，替换内存中存储的被加固软件的明文软件代码所隐藏的对应数据，然后加载明文软件代码。

[0092] 通过本发明实施例提供的被加固软件的认证方法，可获取服务器提供的关键数据，并根据关键数据中的被加固软件的明文软件代码中被隐藏的数据对应的入口地址，能够确定内存中存储的被加固软件的明文软件代码所隐藏的对应数据在明文软件代码中的位置，然后用关键数据中包括的明文软件代码中被隐藏的数据替换内存中存储的被加固软件的明文软件代码所隐藏的对应数据。因此，在本发明实施例提供的被加固软件的认证方法中，被加固软件需要从服务器上获取自身隐藏的关键数据，可以有效地对抗了攻击者的攻击，对该被加固软件有很好的保护作用，而且在获取隐藏的关键数据后，还可以保证该被

加固软件正常运行。

[0093] 其中，如图 1 所示，在本发明实施例中，该认证方法 100 还包括：

[0094] 步骤 S101、计算得到被加固软件的壳程序的完整性校验值，并对壳程序的完整性校验值进行处理，将处理后的处理结果发送给服务器，由服务器对处理结果进行验证，若验证结果为验证通过，则由服务器对关键数据加密处理生成加密数据。

[0095] 因此，在本发明实施例中，在获取关键数据前，首先需要对被加固软件的壳程序的完整性校验值进行验证，只有当验证通过后，才能获取服务器发送的关键数据。另外，通过服务器对被加固软件的壳程序的完整性校验值进行验证，能够有效防止壳程序被篡改，很好地保证其完整性。而且服务器在对被加固软件的壳程序的完整性校验值进行验证过程中，采用基于对称体制的双向挑战应答方式，即由安装于移动终端的被加固软件与服务器双向配合实现，避免了传统的信道攻击，实现了双向实体认证，增加了对被加固软件的壳程序的保护强度。

[0096] 具体地，如图 2 所示，在本发明实施例中，计算得到被加固软件的壳程序的完整性校验值，并对壳程序的完整性校验值进行处理，将处理后的处理结果发送给服务器，由服务器对处理结果进行验证，若验证结果为验证通过，则由服务器对关键数据加密处理生成加密数据（步骤 S101）具体包括：

[0097] 步骤 S1011、将被加固软件的请求信息发送给服务器，由服务器根据被加固软件的请求信息随机生成第一随机数；

[0098] 步骤 S1013、根据第一算法计算得到被加固软件的壳程序的完整性校验值；

[0099] 步骤 S1015、获取第一随机数，将第一随机数与壳程序的完整性校验值进行第一级联处理，获取第一级联结果；

[0100] 步骤 S1017、根据第二算法对第一级联结果进行计算，获取第一计算结果；

[0101] 步骤 S1019、将第一计算结果与被加固软件随机生成的第二随机数进行第二级联处理，并将处理结果发送给服务器，由服务器对处理结果进行验证，若验证结果为验证通过，则由服务器对关键数据加密处理生成加密数据。

[0102] 其中，在本发明实施例中，在对被加固软件的壳程序的完整性校验值进行校验时，首先需要对其壳程序的完整性校验值进行处理，有效地防止了在将壳程序的完整性校验值发送给服务器的过程中遭受到被攻击者修改或者破坏，因此，对被加固软件的壳程序的完整性校验值起到了很好的保护作用。

[0103] 具体地，如图 3 所示，在本发明实施例中，在服务器对被加固软件的壳程序验证通过之后，获取服务器发送的关键数据（步骤 S103），具体包括：

[0104] 步骤 S1031、在服务器对被加固软件的壳程序验证通过之后，对服务器发送的加密数据进行解密运算；

[0105] 步骤 S1033、解密运算完成后，获取解密数据中包含的服务器发送的关键数据。

[0106] 通过对关键数据进行加密处理，能够有效防止服务器发送关键数据的过程中，关键数据被攻击者获取，对关键数据起到了很好的保护作用。因此，被加固软件在获取加密数据后，需要对其进行解密以获取服务器发送的关键数据。

[0107] 具体地，如图 4 所示，在本发明实施例中，根据被隐藏的数据和入口地址，替换内存中存储的被加固软件的明文软件代码所隐藏的对应数据，然后加载明文软件代码（步骤

S105)，具体包括：

[0108] 步骤S1051、根据入口地址，定位被加固软件的明文软件代码所隐藏的对应数据在被加固软件的明文软件代码中的位置；

[0109] 步骤S1053、将被隐藏的数据替换内存中存储的被加固软件的明文软件代码所隐藏的对应数据，然后加载明文软件代码。

[0110] 因此，在获取服务器提供的关键数据后，根据关键数据中的被加固软件的明文软件代码中被隐藏的数据对应的入口地址，能够确定内存中存储的被加固软件的明文软件代码所隐藏的对应数据在明文软件代码中的位置，并用关键数据中包括的明文软件代码中被隐藏的数据替换内存中存储的被加固软件的明文软件代码所隐藏的对应数据。因此，本发明实施例提供的被加固软件的认证方法不仅可以保证该被加固软件正常运行，而且对该被加固软件有很好的保护作用，能够有效地对抗了攻击者的攻击。

[0111] 其中，在本发明实施例中，上述完整性校验值、第一随机数以及第二随机数均采用十六进制表示，当然可以理解的是，在本发明实施例中，对完整性校验值、第一随机数以及第二随机数的表述方式并不进行具体限定。

[0112] 实施例二

[0113] 依据本发明的另一方面，还提供了一种被加固软件的认证方法，应用于一服务器，如图5所示，该认证方法500包括：

[0114] 步骤S501、获取被加固软件发送的处理结果，对被加固软件的壳程序的完整性校验值进行验证；

[0115] 步骤S503、若验证结果为验证通过，则对关键数据进行加密处理，并将加密生成的加密数据发送给被加固软件，关键数据包括：被加固软件的明文软件代码中被隐藏的数据和被隐藏数据对应的入口地址。

[0116] 其中，在本发明实施例中，首先要对被加固软件的壳程序的完整性校验值进行验证，以保证其壳程序的完整性，有效地防止壳程序被篡改，只有当验证通过后，才能向被加固软件发送关键数据，在发送关键数据前，需要对关键数据进行加密处理，因此保证了在发送关键数据过程中的安全性，能够有效防止服务器发送关键数据被攻击者获取，对关键数据起到了很好的保护作用。

[0117] 具体地，如图6所示，在本发明实施例中，根据被加固软件发送的处理结果，对被加固软件的壳程序的完整性校验值进行验证（步骤S501)，具体包括：

[0118] 步骤S5011、获取被加固软件的请求信息，根据请求信息随机生成第一随机数，并将第一随机数发送给被加固软件；

[0119] 步骤S5013、根据被加固软件的请求信息获取被加固软件的ID信息，并根据被加固软件的ID信息获取被加固软件的壳程序的完整性校验值，将第一随机数与壳程序的完整性校验值进行第一级联处理，获取第二级联结果；

[0120] 步骤S5015、根据第二算法对第二级联结果进行计算，得到第二计算结果；

[0121] 步骤S5017、获取被加固软件发送的处理结果，根据处理结果识别获取第一计算结果和第二随机数；

[0122] 步骤S5019、对第一计算结果与第二计算结果进行验证，若第一计算结果与第二计算结果相同，则验证结果为验证通过。

[0123] 由于被加固软件对其壳程序的完整性校验值进行了相应的处理，因此，服务器需要对其获取的被加固软件的壳程序的完整性校验值进行同样的处理，并对被加固软件计算的第一计算结果与服务器计算的第二计算结果进行对比，若第一结果与第二结果不同，则证明被加固软件的壳程序被篡改，遭到攻击者的攻击；若第一计算结果与第二计算结果相同，则被加固软件的壳程序没有被破坏。

[0124] 所以，本发明提供的认证方法能够有效防止壳程序被篡改，很好地保证其完整性，并通过被加固软件与服务器的双向配合，实现了对壳程序完整性的验证，能够避免传统的信道攻击，实现了双向实体认证。其中，上述完整性校验值、第一随机数以及第二随机数均采用十六进制表示，当然可以理解的是，在本发明实施例中，对完整性校验值、第一随机数以及第二随机数的表述方式并不进行具体限定。

[0125] 具体地，如图 7 所示，在本发明实施例中，若验证结果为验证通过，则对关键数据进行加密处理，将加密生成的加密数据发送给被加固软件（步骤 S503），具体包括：

[0126] 步骤 S5031、获取根据第二级联结果识别得到的第二随机数；

[0127] 步骤 S5033、第二随机数与关键数据中包括的被隐藏数据对应的入口地址根据第三算法进行计算，并得到第三计算结果；

[0128] 步骤 S5035、对第三计算结果进行加密处理，将加密后生成的加密数据发送给被加固软件。

[0129] 具体地，在本发明实施例中，将第二随机数与被加固软件的明文软件代码中的入口地址根据第三算法进行计算，具体为：对第二随机数与被加固软件的明文软件代码中的入口地址进行异或的逻辑运算。

[0130] 其中，在本发明实施例中，经过上述加密处理，提高了对关键数据的保护程度，保证了在发送关键数据过程中的安全性，能够有效防止服务器发送关键数据被攻击者获取，对关键数据起到了很好的保护作用。

[0131] 由上述可知，本发明实施例提供的认证方法中的流程不能被逾越，只要在认证过程中出现错误，则不能继续后续流程，因此既能够有效分清服务请求的来源，又能够在恶意应用请求提供服务时，进行有效的保护，大大提高了对被加固软件的保护强度，有效地防止攻击者的攻击，保证被加固软件可以正常运行。

[0132] 实施例三

[0133] 依据本发明的另一个方面，还提供了一种被加固软件的认证装置，应用于一移动终端，如图 8 所示，该认证装置 800 包括：

[0134] 获取模块 803，用于在服务器对被加固软件的壳程序验证通过之后，获取服务器发送的关键数据，关键数据包括：被加固软件的明文软件代码中被隐藏的数据和被隐藏数据对应的入口地址；

[0135] 替换模块 805，用于根据被隐藏的数据和入口地址，替换内存中存储的被加固软件的明文软件代码所隐藏的对应数据，然后加载明文软件代码。

[0136] 其中，如图 8 所示，在本发明实施例中，该认证装置 800 还包括：

[0137] 处理模块 801，用于计算得到被加固软件的壳程序的完整性校验值，并对壳程序的完整性校验值进行处理，将处理后的处理结果发送给服务器，由服务器对处理结果进行验证，若验证结果为验证通过，则由服务器对关键数据加密处理生成加密数据。

[0138] 具体地，如图 9 所示，在本发明实施例中，处理模块 801 具体包括：

[0139] 发送单元 8011，用于将被加固软件的请求信息发送给服务器，由服务器根据被加固软件的请求信息随机生成第一随机数；

[0140] 第一计算单元 8013，用于根据第一算法计算得到被加固软件的壳程序的完整性校验值；

[0141] 第一级联单元 8015，用于获取第一随机数，将第一随机数与壳程序的完整性校验值进行第一级联处理，获取第一级联结果；

[0142] 第二计算单元 8017，用于根据第二算法对第一级联结果进行计算，获取第一计算结果；

[0143] 第二级联单元 8019，用于将第一计算结果与被加固软件随机生成的第二随机数进行第二级联处理，并将处理结果发送给服务器，由服务器对处理结果进行验证，若验证结果为验证通过，则由服务器对关键数据加密处理生成加密数据。

[0144] 具体地，如图 10 所示，在本发明实施例中，获取模块 803 具体包括：

[0145] 解密单元 8031，用于在服务器对被加固软件的壳程序验证通过之后，对服务器发送的加密数据进行解密运算；

[0146] 第一获取单元 8033，用于解密运算完成后，获取解密数据中包含的服务器发送的关键数据。

[0147] 具体地，如图 11 所示，在本发明实施例中，替换模块 805 具体包括：

[0148] 定位单元 8051，用于根据入口地址，定位被加固软件的明文软件代码所隐藏的对应数据在被加固软件的明文软件代码中的位置；

[0149] 替换单元 8053，用于将被隐藏的数据替换内存中存储的被加固软件的明文软件代码所隐藏的对应数据，然后加载明文软件代码。

[0150] 通过本发明实施例提供的被加固软件的认证装置，可获取服务器提供的关键数据，并根据关键数据中的被加固软件的明文软件代码中被隐藏的数据对应的入口地址，能够确定内存中存储的被加固软件的明文软件代码所隐藏的对应数据在明文软件代码中的位置，然后用关键数据中包括的明文软件代码中被隐藏的数据替换内存中存储的被加固软件的明文软件代码所隐藏的对应数据。因此，被加固软件需要从服务器上获取自身隐藏的关键数据，可以有效地对抗了攻击者的攻击，对该被加固软件有很好的保护作用，而且在获取隐藏的关键数据后，还可以保证该被加固软件正常运行。

[0151] 实施例四

[0152] 依据本发明的另一方面，还提供了一种被加固软件的认证装置，应用于一服务器，如图 12 所示，该认证装置 1200 包括：

[0153] 验证模块 1201，用于获取被加固软件发送的处理结果，对被加固软件的壳程序的完整性校验值进行验证；

[0154] 加密模块 1203，用于若验证结果为验证通过，则对关键数据进行加密处理，将加密生成的加密数据发送给被加固软件，关键数据包括：被加固软件的明文软件代码中被隐藏的数据和被隐藏数据对应的入口地址。

[0155] 具体地，如图 13 所示，在本发明实施例中，验证模块 1201 具体包括：

[0156] 生成单元 12011，用于获取被加固软件的请求信息，根据请求信息随机生成第一随

机数，并将第一随机数发送给被加固软件；

[0157] 第三级联单元 12013，用于根据被加固软件的请求信息获取被加固软件的 ID 信息，并根据被加固软件的 ID 信息获取被加固软件的壳程序的完整性校验值，将第一随机数与壳程序的完整性校验值进行第一级联处理，获取第二级联结果；

[0158] 第三计算单元 12015，用于根据第二算法对第二级联结果进行计算，得到第二计算结果；

[0159] 识别单元 12017，用于获取被加固软件发送的处理结果，根据处理结果识别获取第一计算结果和第二随机数；

[0160] 验证单元 12019，用于对第一计算结果与第二计算结果进行验证，若第一计算结果与第二计算结果相同，则验证结果为验证通过。

[0161] 具体地，如图 14 所示，在本发明实施例中，添加模块 1203 具体包括：

[0162] 第二获取单元 12031，用于获取根据第二级联结果识别得到的第二随机数；

[0163] 第四计算单元 12033，用于第二随机数与关键数据中包括的被隐藏数据对应的入口地址根据第三算法进行计算，并得到第三计算结果；

[0164] 加密单元 12035，用于对第三计算结果进行加密处理，将加密后生成的加密数据发送给被加固软件。

[0165] 其中，第四计算单元 12033 在根据第三算法进行计算时，具体为：

[0166] 对第二随机数与被加固软件的明文软件代码中的入口地址进行异或的逻辑运算。

[0167] 本发明实施例提供的认证装置首先要对被加固软件的壳程序的完整性校验值进行验证，以保证其壳程序的完整性，有效地防止壳程序被篡改，然后在当验证通过后，向被加固软件发送关键数据，其中在发送关键数据前，需要对关键数据进行加密处理，因此保证了在发送关键数据过程中的安全性，能够有效防止服务器发送关键数据被攻击者获取，对关键数据起到了很好的保护作用。

[0168] 以上所述的是本发明的优选实施方式，应当指出对于本技术领域的普通人员来说，在不脱离本发明所述的原理前提下还可以作出若干改进和润饰，这些改进和润饰也在本发明的保护范围内。

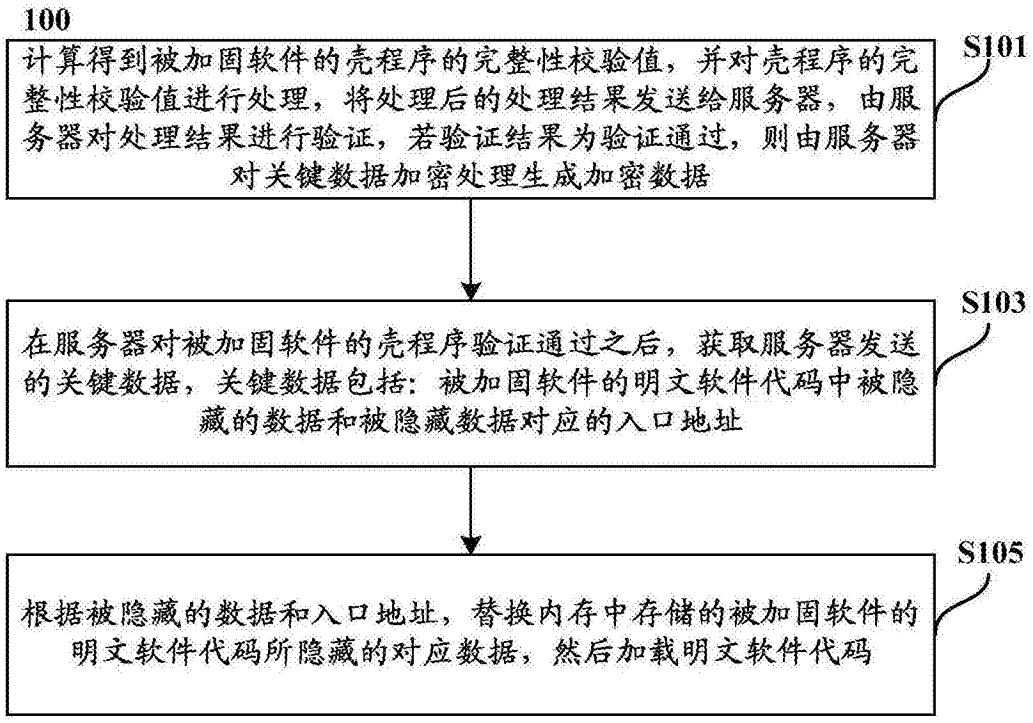

100
计算得到被加固软件的壳程序的完整性校验值，并对壳程序的完整性校验值进行处理，将处理后的处理结果发送给服务器，由服务器对处理结果进行验证，若验证结果为验证通过，则由服务器对关键数据加密处理生成加密数据
S101
在服务器对被加固软件的壳程序验证通过之后，获取服务器发送的关键数据，关键数据包括：被加固软件的明文软件代码中被隐藏的数据和被隐藏数据对应的入口地址
S103
根据被隐藏的数据和入口地址，替换内存中存储的被加固软件的明文软件代码所隐藏的对应数据，然后加载明文软件代码
S105

图 1

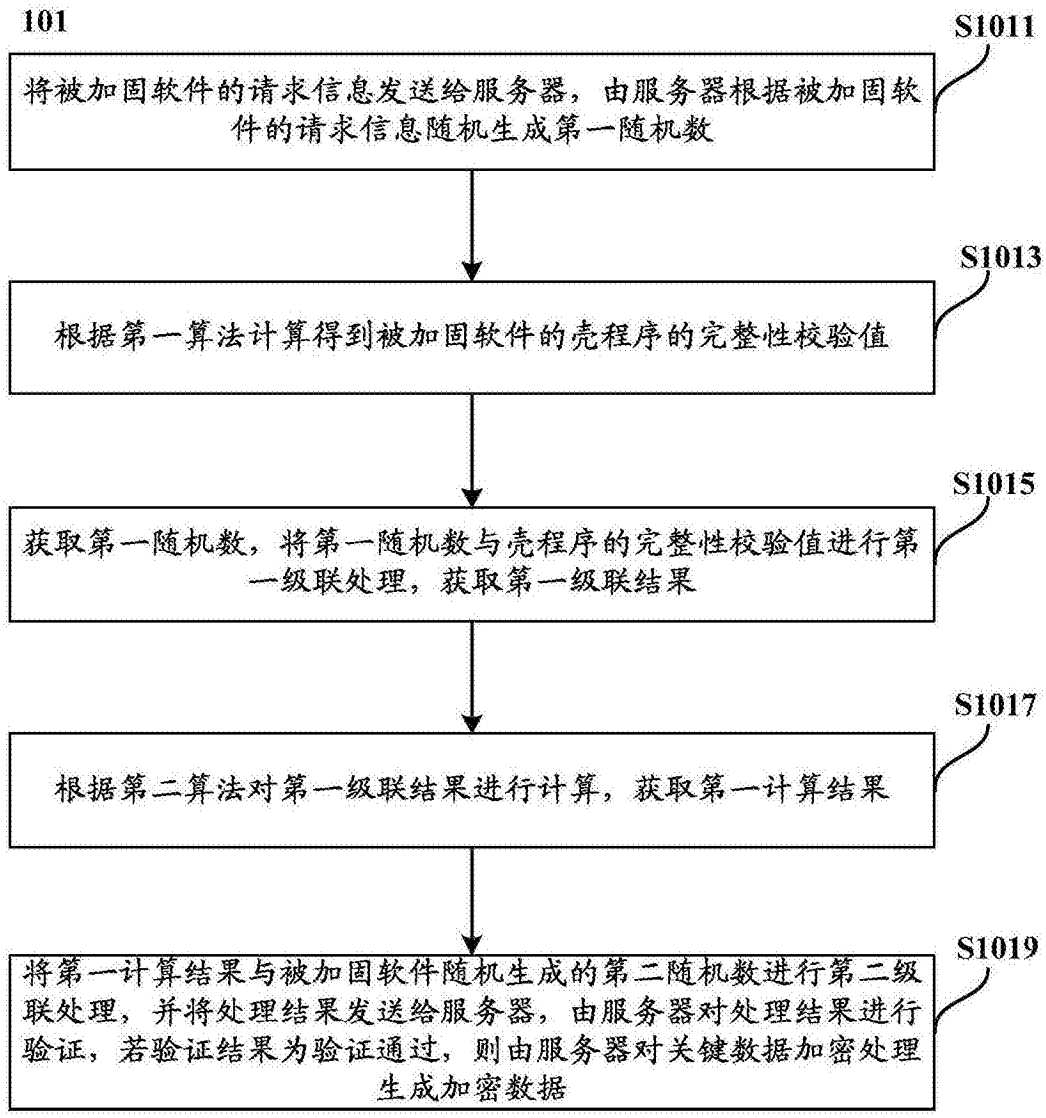

101
S1011
将被加固软件的请求信息发送给服务器，由服务器根据被加固软件的请求信息随机生成第一随机数
S1013
根据第一算法计算得到被加固软件的壳程序的完整性校验值
S1015
获取第一随机数，将第一随机数与壳程序的完整性校验值进行第一级联处理，获取第一级联结果
S1017
根据第二算法对第一级联结果进行计算，获取第一计算结果
S1019
将第一计算结果与被加固软件随机生成的第二随机数进行第二级联处理，并将处理结果发送给服务器，由服务器对处理结果进行验证，若验证结果为验证通过，则由服务器对关键数据加密处理生成加密数据

图 2

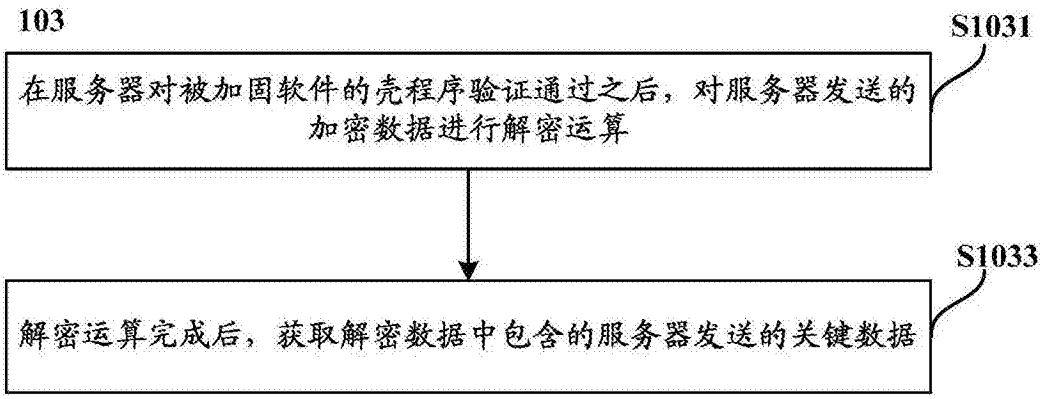

103
S1031
在服务器对被加固软件的壳程序验证通过之后，对服务器发送的加密数据进行解密运算
S1033
解密运算完成后，获取解密数据中包含的服务器发送的关键数据

图 3

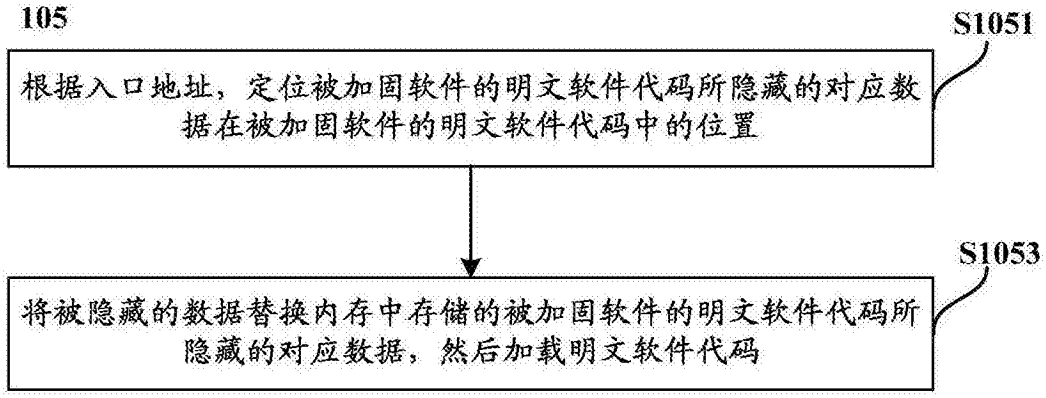

105
S1051
根据入口地址，定位被加固软件的明文软件代码所隐藏的对应数据在被加固软件的明文软件代码中的位置
S1053
将被隐藏的数据替换内存中存储的被加固软件的明文软件代码所隐藏的对应数据，然后加载明文软件代码

图 4

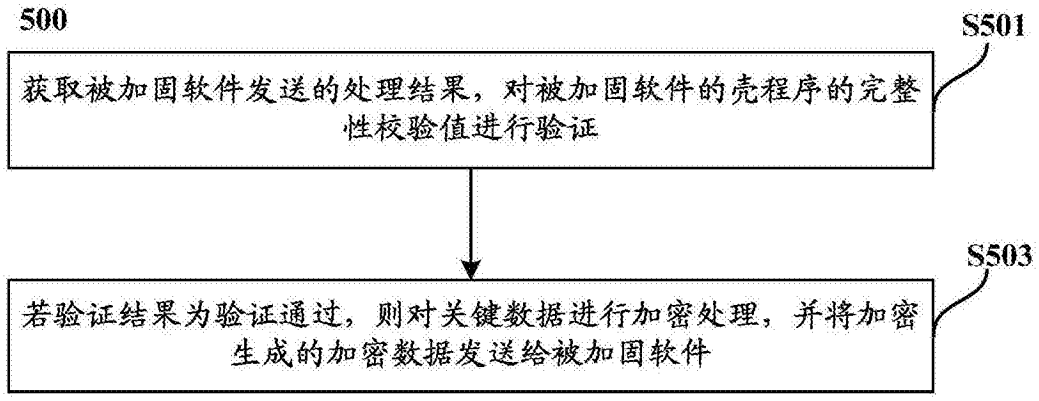

500
S501
获取被加固软件发送的处理结果，对被加固软件的壳程序的完整性校验值进行验证
S503
若验证结果为验证通过，则对关键数据进行加密处理，并将加密生成的加密数据发送给被加固软件

图 5

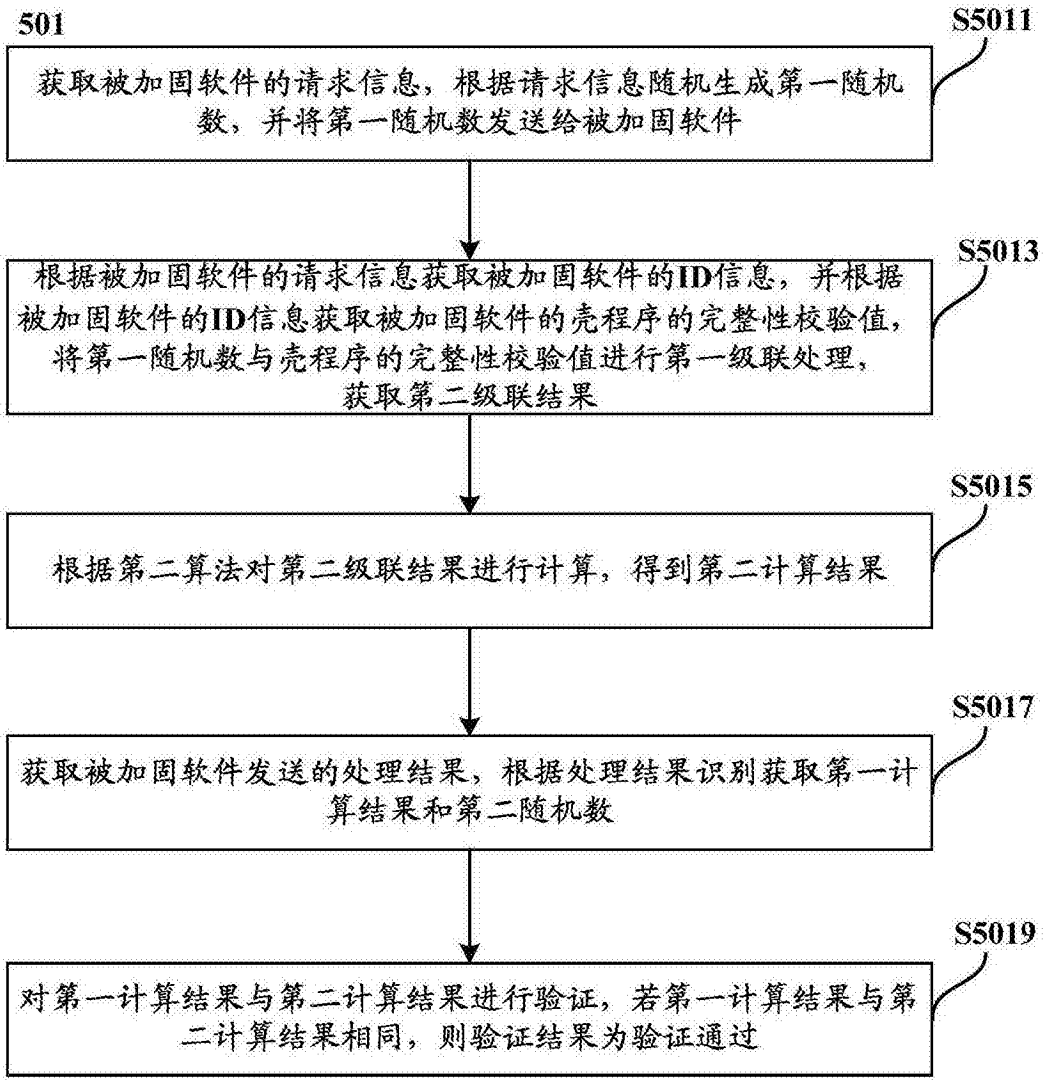

501
S5011
获取被加固软件的请求信息，根据请求信息随机生成第一随机数，并将第一随机数发送给被加固软件
S5013
根据被加固软件的请求信息获取被加固软件的ID信息，并根据被加固软件的ID信息获取被加固软件的壳程序的完整性校验值，将第一随机数与壳程序的完整性校验值进行第一级联处理，获取第二级联结果
S5015
根据第二算法对第二级联结果进行计算，得到第二计算结果
S5017
获取被加固软件发送的处理结果，根据处理结果识别获取第一计算结果和第二随机数
S5019
对第一计算结果与第二计算结果进行验证，若第一计算结果与第二计算结果相同，则验证结果为验证通过

图 6

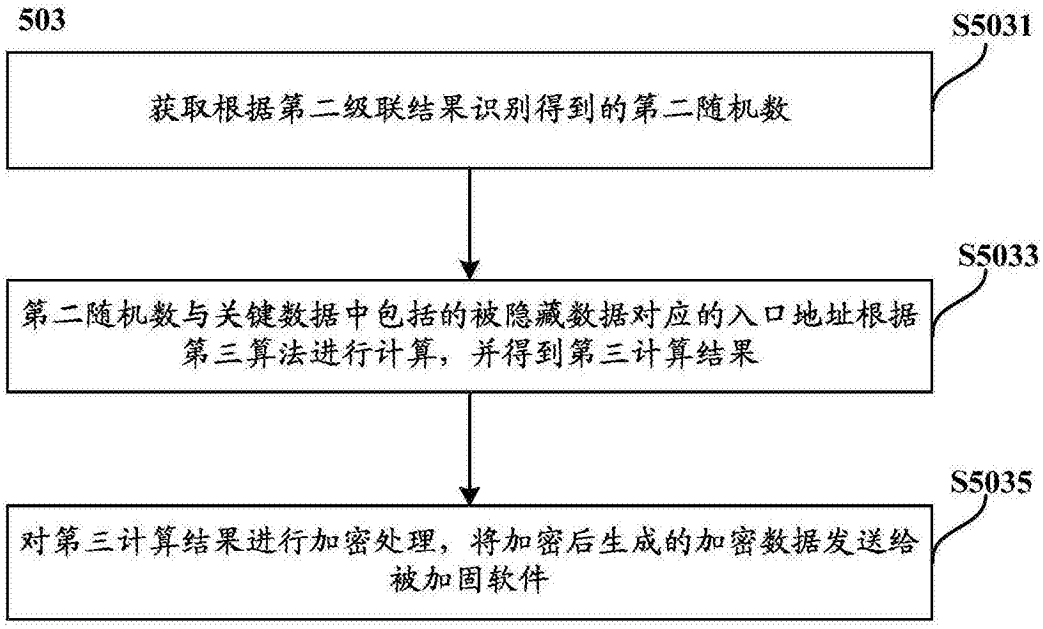

503
S5031
获取根据第二级联结果识别得到的第二随机数
S5033
第二随机数与关键数据中包括的被隐藏数据对应的入口地址根据第三算法进行计算，并得到第三计算结果
S5035
对第三计算结果进行加密处理，将加密后生成的加密数据发送给被加固软件

图 7

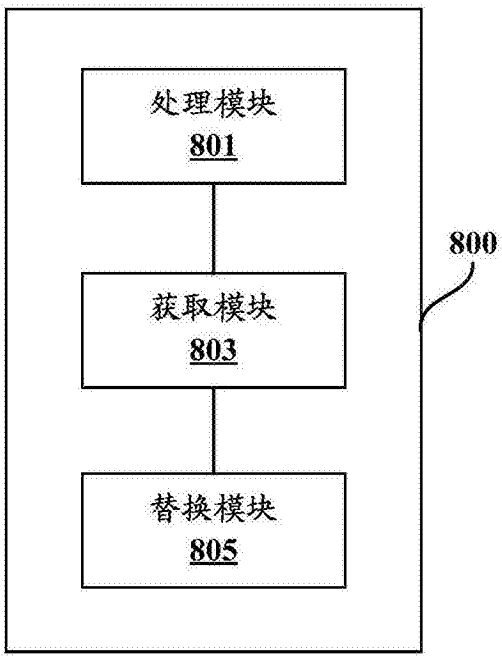

处理模块
801
800
获取模块
803
替换模块
805

图 8

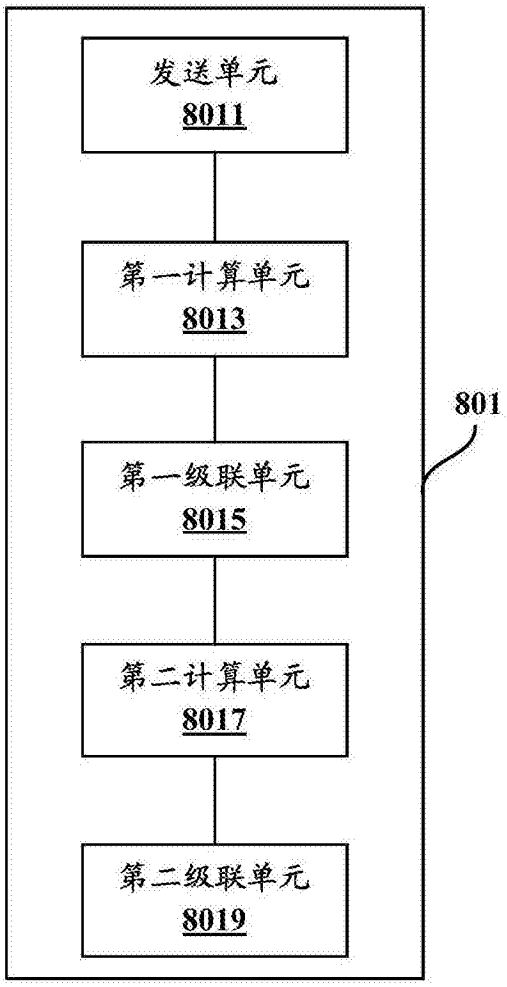


图 9

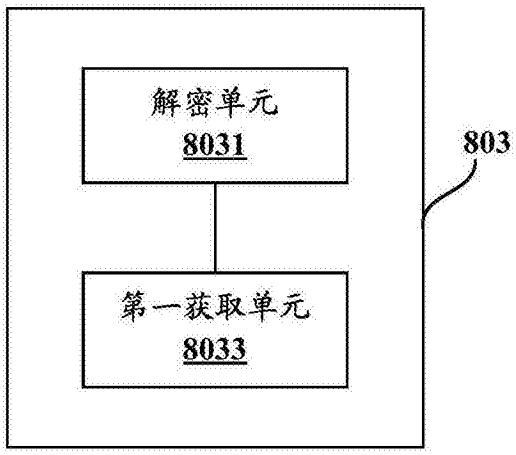


图 10

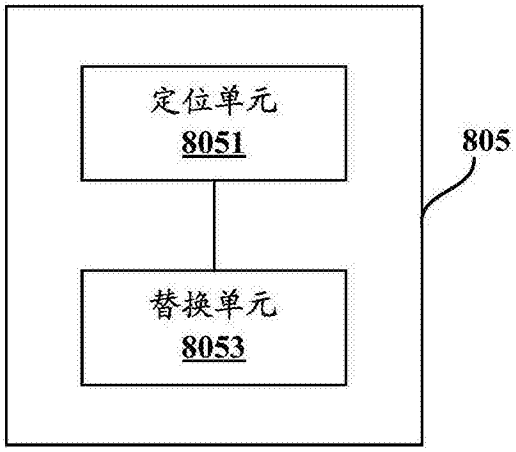


图 11

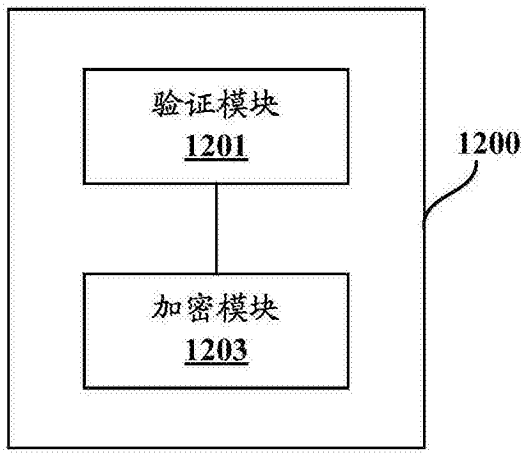


图 12

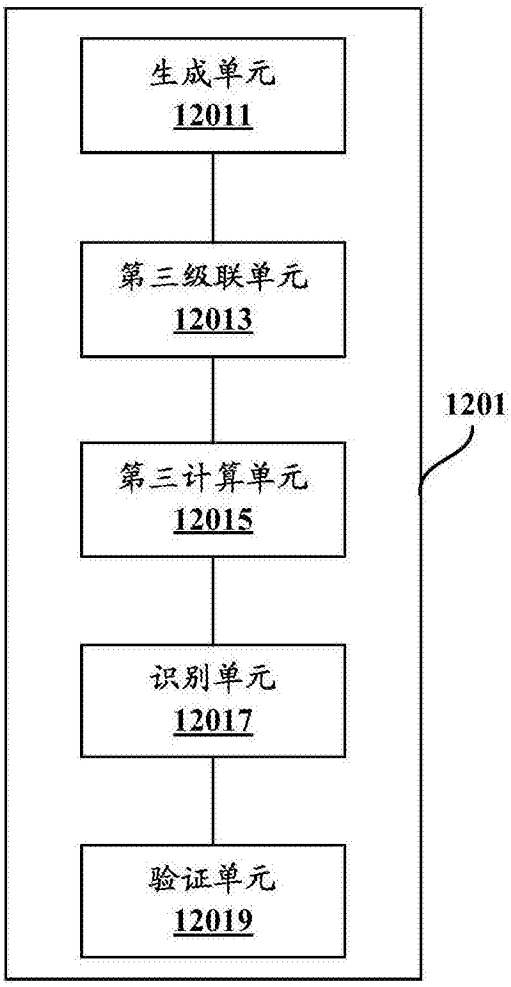

生成单元
12011
第三级联单元
12013
第三计算单元
12015
识别单元
12017
验证单元
12019
1201

图 13

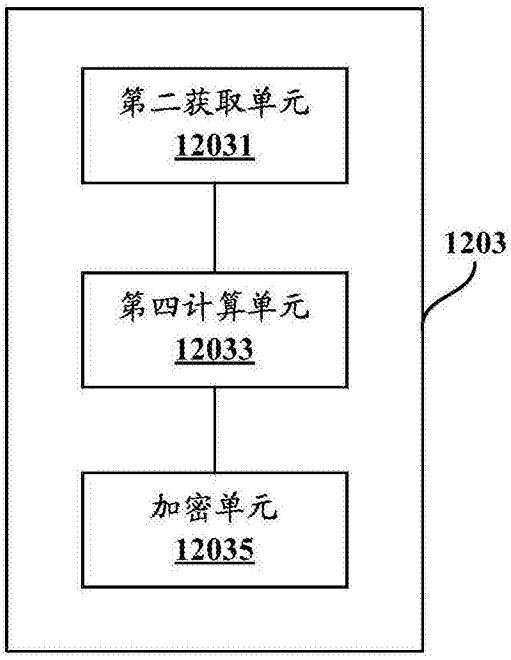

第二获取单元
12031
第四计算单元
12033
加密单元
12035
1203

图 14