(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 107408166 A
(43)申请公布日 2017.11.28

(21)申请号 201680015591.7

(22)申请日 2016.03.14

(30)优先权数据
10-2015-0035177 2015.03.13 KR

(85)PCT国际申请进入国家阶段日
2017.09.13

(86)PCT国际申请的申请数据
PCT/KR2016/002537 2016.03.14

(87)PCT国际申请的公布数据
WO2016/148473 KO 2016.09.22

(71)申请人 爱维斯宾公司
地址 韩国首尔市
申请人 河英彬

(72)发明人 河英彬

(74)专利代理机构 北京金律言科知识产权代理事务所(普通合伙) 11461
代理人 罗延红 姚远达

(51)Int.Cl.
G06F 21/12(2013.01)
G06F 21/44(2013.01)
G06F 21/51(2013.01)
G06F 21/57(2013.01)

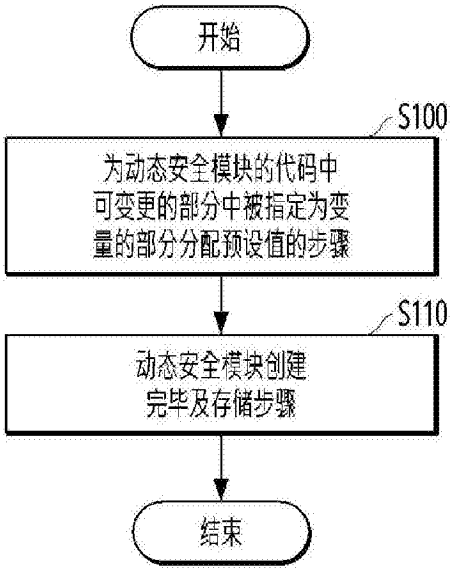
权利要求书2页 说明书13页 附图5页

(54)发明名称

动态安全模块创建方法及创建装置

(57)摘要

本发明揭示了一种动态安全模块创建方法及创建装置，构成上述动态安全模块的代码中可变更的部分的一部分或全部被指定为变量，为变量中的至少一个以上分配预设值，让代码的一部分或全部代码具备有效期。



CN 107408166 A

1.一种动态安全模块的创建方法，其以让在用户终端为了安全而执行的代码在每次执行时都不相同的方式创建分配给上述用户终端的动态安全模块，其特征在于，

包括下列步骤，亦即，构成上述动态安全模块的代码中可变更的部分的一部分或全部被指定为变量，为上述变量中的至少一个以上分配预设值；

构成传输到上述用户终端的动态安全模块的代码的一部分或全部代码具备有效期。

2.根据权利要求1所述的动态安全模块的创建方法，其特征在于，

上述动态安全模块的可变更部分是能够把从代码的函数名、指定拟运行的算法的变量、协议字段、指定协议序列的变量、指定编译级别的变量及指定执行代码混淆方法的变量所构成的群选择的1种以上要素予以变更的代码。

3.根据权利要求1所述的动态安全模块的创建方法，其特征在于，

上述有效期是一种上述有效期截止时删除上述代码的一部分或全部代码或者禁止使用上述代码的一部分或全部代码的有效期。

4.根据权利要求1所述的动态安全模块的创建方法，其特征在于，

上述创建方法还包括下列步骤：

和上述用户终端的安全客户端创建安全会话；及

把上述动态安全模块传输给创建了上述安全会话的用户终端的安全客户端。

5.根据权利要求4所述的动态安全模块的创建方法，其特征在于，

上述创建方法还包括下列步骤：从传输给上述安全客户端的动态安全模块接收安全管理结果并且确认所收到的上述安全管理结果，然后把安全管理确认结果值传输给上述安全客户端的动态安全模块。

6.根据权利要求4所述的动态安全模块的创建方法，其特征在于，

上述创建方法还包括下列步骤：上述用户终端发生安全问题时，把命令上述用户终端的应用程序停止的停止指令传输给上述安全客户端的动态安全模块。

7.根据权利要求4所述的动态安全模块的创建方法，其特征在于，

上述创建方法创建作为安全会话标识符的会话ID并加以存储，把上述会话ID传输给上述安全客户端让上述安全客户端存储上述会话ID而创建上述安全会话。

8.根据权利要求4所述的动态安全模块的创建方法，其特征在于，

上述创建方法还包括下列步骤：

在维持着上述安全会话的期间让关于传输到上述安全客户端的各个上述动态安全模块的参数被存储。

9.根据权利要求8所述的动态安全模块的创建方法，其特征在于，

上述创建方法还包括下列步骤：

验证上述安全客户端所传输过来的详细信息是否和上述动态安全模块的参数的配置相同。

10.一种动态安全模块创建装置，该装置以让在用户终端为了安全而执行的代码在每次执行时都不相同的方式创建分配给上述用户终端的动态安全模块，其特征在于，

包括：

通信单元，通过网络收发安全管理事件；及

处理器，控制上述通信单元；

上述处理器让构成上述动态安全模块的代码中可变更的部分的一部分或全部被指定为变量，为上述变量中至少一个以上分配预设值，让构成传输到上述用户终端的动态安全模块的代码的一部分或全部代码具备有效期。

11.根据权利要求10所述的动态安全模块创建装置，其特征在于，

上述动态安全模块的可变更部分是能够把从代码的函数名、指定拟运行的算法的变量、协议字段、指定协议序列的变量、指定编译级别的变量及指定执行代码混淆方法的变量所构成的群选择的1种以上的要素予以变更的代码。

12.根据权利要求10所述的动态安全模块创建装置，其特征在于，

上述处理器和上述用户终端的安全客户端创建安全会话，把上述动态安全模块传输给创建了上述安全会话的用户终端的安全客户端。

13.根据权利要求12所述的动态安全模块创建装置，其特征在于，

上述处理器从传输给上述安全客户端的动态安全模块接收安全管理结果并且确认所收到的上述安全管理结果，然后把安全管理确认结果值传输给上述安全客户端的动态安全模块。

14.根据权利要求12所述的动态安全模块创建装置，其特征在于，

上述处理器在上述用户终端发生安全问题时，把命令上述用户终端的应用程序停止的停止指令传输给上述安全客户端的动态安全模块。

15.根据权利要求12所述的动态安全模块创建装置，其特征在于，

上述处理器创建作为安全会话标识符的会话ID并加以存储，把上述会话ID传输给上述安全客户端让上述安全客户端存储上述会话ID而创建上述安全会话。

16.根据权利要求12所述的动态安全模块创建装置，其特征在于，

上述处理器在维持着上述安全会话的期间让关于传输到上述安全客户端的各个上述动态安全模块的参数被存储。

17.根据权利要求12所述的动态安全模块创建装置，其特征在于，

上述处理器验证上述安全客户端所传输过来的详细信息是否和上述动态安全模块的参数的配置相同。

18.根据权利要求10所述的动态安全模块创建装置，其特征在于，

上述动态安全模块创建装置还包括存储器，该存储器存储拟传输给上述用户终端的安全客户端的动态安全模块、作为安全会话标识符的会话ID及关于动态安全模块的参数。

19.一种计算机可读存储介质，其特征在于，

其记录了下列程序，该程序用于执行权利要求1到9中某一项的创建方法。

动态安全模块创建方法及创建装置

技术领域

[0001] 本发明涉及一种动态安全模块创建装置及创建方法，更详细地说，该动态安全模块创建装置及创建方法创建了执行安全管理的源代码的一部分或全部代码具备预定的有效期的动态安全模块后传输给用户终端的安全客户端，让针对用户终端的各种应用程序的安全模块随时更新，因此让针对应用程序的破解变得困难而得以显著地提高用户终端的安全性(security)。

背景技术

[0002] 近来，作为移动终端的智能手机在现代生活中已成为不可或缺的必需品并且在全世界范围内广泛普及。但是，智能手机在安全方面的脆弱性被陆续发现而使得恶意应用程序的攻击急剧增加。

[0003] 黑客以移动终端为对象开发恶意应用程序并且插入恶意代码后通过公开市场或互联网将其伪装成正常应用程序发行给一般用户。恶意应用程序被存储到移动终端时，移动终端内的恶意应用程序可能会在用户不知情的状况下进行攻击把SMS收发信息、电话号码簿、互联网接入记录之类的的个人信息、以及用于手机银行等用途的移动公认认证书之类的金融信息泄露到外部服务器。

[0004] 大部分的应用程序安全解决方案在执行了应用程序后和应用程序的安全模块进行通信呼叫安全逻辑并且将其结果予以响应。但黑客攻击导致其和安全模块之间的通信被强制中断或者伪变造的应用程序导致安全模块丧失其能力的话，个人私密信息及金融相关的个人信息就会发生致命的脆弱性。

[0005] 因此，近来迫切需要开发出能够在海内外广泛普及的基于移动终端的用户环境下解决安全脆弱问题并且提高用户终端所含众多软件的安全性的技术。

发明内容

[0006] 技术问题

[0007] 本发明旨在解决上述现有技术的问题，本发明的目的是提供一种动态安全模块创建方法及创建装置，该动态安全模块创建方法及创建装置创建了执行安全管理的源代码的一部分或全部代码具备预定的有效期的动态安全模块后传输给用户终端的安全客户端，让针对用户终端的各种应用程序的安全模块随时更新，因此让针对应用程序的破解变得困难而得以显著地提高用户终端的安全性(security)。

[0008] 解决问题的手段

[0009] 为了达到该目的，本发明揭示了一种动态安全模块的创建方法，其以让在用户终端为了安全而执行的代码在每次执行时都不相同的方式创建分配给上述用户终端的动态安全模块，其包括下列步骤，亦即，构成上述动态安全模块的代码中可变更的部分的一部分或全部被指定为变量，为上述变量中的至少一个以上分配预设值。构成传输到上述用户终端的动态安全模块的代码的一部分或全部代码具备有效期。

[0010] 上述动态安全模块的可变更部分可以是能够把从代码的函数名、指定拟运行的算法的变量、协议字段、指定协议序列的变量、指定编译级别的变量及指定执行代码混淆方法的变量所构成的群选择的1种以上的要素予以变更的代码。

[0011] 上述有效期可以是一种上述有效期截止时删除上述代码的一部分或全部代码或者禁止使用上述代码的一部分或全部代码的有效期。

[0012] 上述创建方法还包括下列步骤：和上述用户终端的安全客户端创建安全会话；及把上述动态安全模块传输给创建了上述安全会话的用户终端的安全客户端。

[0013] 上述创建方法还包括下列步骤：从传输给上述安全客户端的动态安全模块接收安全管理结果并且确认所收到的上述安全管理结果，然后把安全管理确认结果值传输给上述安全客户端的动态安全模块。

[0014] 上述创建方法还包括下列步骤：上述用户终端发生安全问题时，把命令上述用户终端的应用程序停止的停止指令传输给上述安全客户端的动态安全模块。

[0015] 上述创建方法创建作为安全会话标识符的会话ID并加以存储，把上述会话ID传输给上述安全客户端让上述安全客户端存储上述会话ID而创建上述安全会话。

[0016] 上述创建方法还包括下列步骤：在维持着上述安全会话的期间让关于传输到上述安全客户端的各个上述动态安全模块的参数被存储。

[0017] 上述创建方法还包括下列步骤：验证上述安全客户端所传输过来的详细信息是否和上述动态安全模块的参数的配置相同。

[0018] 而且，为了达到上述目的，本发明揭示了一种动态安全模块创建装置，该装置以让在用户终端为了安全而执行的代码在每次执行时都不相同的方式创建分配给上述用户终端的动态安全模块，其包括：通信单元，通过网络收发安全管理事件；及处理器，控制上述通信单元；上述处理器让构成上述动态安全模块的代码中可变更的部分的一部分或全部被指定为变量，为上述变量中至少一个以上分配预设值，让构成传输到上述用户终端的动态安全模块的代码的一部分或全部代码具备有效期。

[0019] 上述动态安全模块的可变更部分可以是能够把从代码的函数名、指定拟运行的算法的变量、协议字段、指定协议序列的变量、指定编译级别的变量及指定执行代码混淆方法的变量所构成的群选择的1种以上的要素予以变更的代码。

[0020] 上述处理器则和上述用户终端的安全客户端创建安全会话，把上述动态安全模块传输给创建了上述安全会话的用户终端的安全客户端

[0021] 上述处理器从传输给上述安全客户端的动态安全模块接收安全管理结果并且确认所收到的上述安全管理结果，然后把安全管理确认结果值传输给上述安全客户端的动态安全模块。

[0022] 上述处理器在上述用户终端发生安全问题时，把命令上述用户终端的应用程序停止的停止指令传输给上述安全客户端的动态安全模块。

[0023] 上述处理器创建作为安全会话标识符的会话ID并加以存储，把上述会话ID传输给上述安全客户端让上述安全客户端存储上述会话ID而创建上述安全会话。

[0024] 上述处理器在维持着上述安全会话的期间让关于传输到上述安全客户端的各个上述动态安全模块的参数被存储。

[0025] 上述处理器验证上述安全客户端所传输过来的详细信息是否和上述动态安全模

块的参数的配置相同。

[0026] 上述动态安全模块创建装置还包括存储器，该存储器存储拟传输给上述用户终端的安全客户端的动态安全模块、作为安全会话标识符的会话ID及关于动态安全模块的参数。

[0027] 而且，为了达到上述目的，本发明揭示了一种计算机可读存储介质，其记录了下列程序，该程序用于执行上述动态安全模块创建方法。

[0028] 发明效果

[0029] 本发明的动态安全模块创建方法及创建装置创建了执行安全管理的源代码的一部分或全部代码具备预定的有效期的动态安全模块后传输给用户终端的安全客户端，让针对用户终端的各种应用程序的安全模块随时更新，因此让针对应用程序的破解变得困难而得以显著地提高用户终端的安全性(security)。

附图说明

[0030] 图1是示出本发明第一实施例的动态安全模块创建方法的顺序的方块图。

[0031] 图2是示出本发明第二实施例的动态安全模块创建方法的顺序的方块图。

[0032] 图3是示出本发明的动态安全模块创建装置的概略配置的模式图。

[0033] 图4是示出本发明的一个实施例的动态安全模块创建方法中由相异的函数构成的动态代码创建例的模式图。

[0034] 图5是示出本发明的一个实施例的动态安全模块创建方法中由相异的算法构成的动态算法创建例的模式图。

[0035] 图6是示出本发明的一个实施例的动态安全模块创建方法中具备相异的编译级别的动态编译参数创建例的模式图。

[0036] 图7是示出本发明的一个实施例的动态安全模块创建方法中会话ID及动态安全模块参数创建例的模式图。

[0037] 图8是示出本发明的一个实施例的动态安全模块创建方法中动态安全模块协议字段创建例的模式图。

[0038] 图9是示出本发明的一个实施例的动态安全模块创建方法中动态安全模块协议序列创建例的模式图。

[0039] 最佳实施方式

[0040] 为了达到该目的，本发明揭示了一种动态安全模块的创建方法，以让在用户终端为了安全而执行的代码在每次执行时都不相同的方式创建分配给上述用户终端的动态安全模块，该方法包括下列步骤，亦即，构成上述动态安全模块的代码中可变更的部分的一部分或全部被指定为变量，为上述变量中的至少一个以上分配预设值；构成传输到上述用户终端的动态安全模块的代码的一部分或全部代码具备有效期。

[0041] 上述动态安全模块的可变更部分可以是能够把从代码的函数名、指定拟运行的算法的变量、协议字段、指定协议序列的变量、指定编译级别的变量及指定执行代码混淆方法的变量所构成的群选择的1种以上的要素予以变更的代码。

[0042] 上述有效期可以是一种上述有效期截止时删除上述代码的一部分或全部代码或者禁止使用上述代码的一部分或全部代码的有效期。

[0043] 上述创建方法还包括下列步骤:和上述用户终端的安全客户端创建安全会话;及把上述动态安全模块传输给创建了上述安全会话的用户终端的安全客户端。

[0044] 上述创建方法还包括下列步骤:从传输给上述安全客户端的动态安全模块接收安全管理结果并且确认所收到的上述安全管理结果,然后把安全管理确认结果值传输给上述安全客户端的动态安全模块。

[0045] 上述创建方法还包括下列步骤:上述用户终端发生安全问题时,把命令上述用户终端的应用程序停止的停止指令传输给上述安全客户端的动态安全模块。

[0046] 上述创建方法创建作为安全会话标识符的会话ID并加以存储,把上述会话ID传输给上述安全客户端让上述安全客户端存储上述会话ID而创建上述安全会话。

[0047] 上述创建方法还包括下列步骤:在维持着上述安全会话的期间让关于传输到上述安全客户端的各个上述动态安全模块的参数被存储。

[0048] 上述创建方法还包括下列步骤:验证上述安全客户端所传输过来的详细信息是否和上述动态安全模块的参数的配置相同。

[0049] 而且,为了达到上述目的,本发明揭示了一种动态安全模块创建装置,该装置以让在用户终端为了安全而执行的代码在每次执行时都不相同的方式创建分配给上述用户终端的动态安全模块,其包括:通信单元,通过网络收发安全管理事件;及处理器,控制上述通信单元;上述处理器让构成上述动态安全模块的代码中可变更的部分的一部分或全部被指定为变量,为上述变量中至少一个以上分配预设值,让构成传输到上述用户终端的动态安全模块的代码的一部分或全部代码具备有效期。

[0050] 上述动态安全模块的可变更部分可以是能够把从代码的函数名、指定拟运行的算法的变量、协议字段、指定协议序列的变量、指定编译级别的变量及指定执行代码混淆方法的变量所构成的群选择的1种以上的要素予以变更的代码。

[0051] 上述处理器则和上述用户终端的安全客户端创建安全会话,把上述动态安全模块传输给创建了上述安全会话的用户终端的安全客户端。

[0052] 上述处理器从传输给上述安全客户端的动态安全模块接收安全管理结果并且确认所收到的上述安全管理结果,然后把安全管理确认结果值传输给上述安全客户端的动态安全模块。

[0053] 上述处理器在上述用户终端发生安全问题时,把命令上述用户终端的应用程序停止的停止指令传输给上述安全客户端的动态安全模块。

[0054] 上述处理器创建作为安全会话标识符的会话ID并加以存储,把上述会话ID传输给上述安全客户端让上述安全客户端存储上述会话ID而创建上述安全会话。

[0055] 上述处理器在维持着上述安全会话的期间让关于传输到上述安全客户端的各个上述动态安全模块的参数被存储。

[0056] 上述处理器验证上述安全客户端所传输过来的详细信息是否和上述动态安全模块的参数的配置相同。

[0057] 上述动态安全模块创建装置还包括存储器,该存储器存储拟传输给上述用户终端的安全客户端的动态安全模块、作为安全会话标识符的会话ID及关于动态安全模块的参数。

[0058] 而且,为了达到上述目的,本发明揭示了一种计算机可读存储介质,其记录了下列

程序，该程序用于执行上述动态安全模块创建方法。

具体实施方式

[0059] 下面结合附图详细说明本发明的优选实施例。在说明本发明之前，如果认为对于公知结构或功能的相关说明可能会非必要地混淆本发明的主旨，将省略其详细说明。而且，在说明本发明的实施例时的具体数值只是实施例而已。

[0060] 图1示出了显示本发明第一实施例的动态安全模块创建方法的顺序的方块图，图2示出了显示本发明第二实施例的动态安全模块创建方法的顺序的方块图。

[0061] 请参阅这些附图，本发明第一实施例的动态安全模块的创建方法以让在用户终端为了安全而执行的代码在每次执行时都不相同的方式创建分配给上述用户终端的动态安全模块，该方法包括下列步骤：构成上述动态安全模块的代码中可变更的部分的一部分或全部被指定为变量，为上述变量中的至少一个以上分配预设值(S100)，让构成传输到上述用户终端的动态安全模块的代码的一部分或全部代码具备有效期地创建上述动态安全模块并且加以存储(S110)。

[0062] 亦即，本发明的动态安全模块创建方法包括下列步骤：在构成动态安全模块的代码中可变更的部分的一部分或全部被指定为变量的动态安全模块中为上述变量中的至少一个以上分配预设值的步骤；因此在上述用户终端的安全客户端执行安全管理的代码被动态随机地选择而让黑客很难破解动态安全模块，进而能够显著地提高加载了动态安全模块的用户终端的安全性。

[0063] 而且，使得在用户终端的安全客户端经常被更新并执行安全管理的动态安全模块的代码配置相异，从而能够创建具备无数种类的代码的相异动态安全模块。

[0064] 具体地说，包括下列步骤，亦即，使用在上述用户终端的安全客户端执行安全管理的各个功能的代码中可变更的部分的一部分或全部被指定为变量的代码并且为上述变量中的至少一个以上分配预设值，因此能够创建无数种类的动态安全模块。

[0065] 例如，由于使用了把动态安全模块的可变更的代码中一部分r或全部n指定为变量的代码，因此能根据如下所述的组合公式制作多个可变更的代码的组合nCr后使用。

[0066] $$nCr=\frac{n(n-1)(n-2)...(n-r+1)}{r(r-1)(r-2)...\cdot 2\cdot 1}=\frac{n!}{r!(n-1)!}$$

[0067] 在此，r为n≥r.

[0068] 而且，利用关于被存储在下述装置的可变更的代码的多种代码a为被指定为变量的代码分配预设值的话，所分配的值b的种类能以下述组合aCb生成，该装置执行上述动态安全模块创建方法。

[0069] $$aCb=\frac{a(a-1)(a-2)...(a-b+1)}{b(b-1)(b-2)...\cdot 2\cdot 1}=\frac{a!}{b!(a-b)!}$$

[0070] 在此，b为a≥b。

[0071] 因此，上述动态安全模块的创建方法具有下列特征，亦即，能以无数的种类创建出在用户终端为了安全而执行的代码。

[0072] 而且，上述动态安全模块由于传输到用户终端的动态安全模块的代码的一部分或全部代码具备有效期地配置而得以让传输到上述用户终端的安全客户端的动态安全模块

经常更新，从而能够有效地防止因安全模块被破解或感染病毒而导致加载到用户终端的应用程序发生安全问题的现象。

[0073] 作为一例，上述动态安全模块的可变更部分可以是能够把从代码的函数名、指定拟运行的算法的变量、协议字段、指定协议序列的变量、指定编译级别的变量及指定执行代码混淆方法的变量所构成的群选择的1种以上的要素予以变更的代码。

[0074] 亦即，对于构成在上述用户终端安全客户端为了安全管理而驱动的动态安全模块的代码中像实现驱动起始点的代码一样即使动态安全模块从新更新也不会跟着改变而固定的代码以外的其余可变更的代码，把从代码的函数名、指定拟运行的算法的变量、协议字段、指定协议序列的变量、指定编译级别的变量及指定执行代码混淆方法的变量所构成的群选择的1种以上的要素予以变更而得以创建无数种类的动态安全模块。

[0075] 在此，上述协议字段是对于上述动态安全模块在上述安全客户端执行的安全管理的各式各样项目的执行方法之类的规约，例如，其可以是把能够对包含上述安全客户端的应用程序构成破解威胁的要素的存在与否进行判别的结果加以传输的通信规约，也可以是把对于上述应用程序的病毒、Boot&file病毒等的自我治疗详细信息加以传输的通信规约。

[0076] 而且，上述协议序列指的是包含上述动态安全模块118在上述安全客户端执行的管理在内的众多项目的执行顺序，作为一例，在针对安装了上述应用程序的终端机的O/S伪变造、应用程序(App)的伪变造、获取最高权限(Rooting)、调试程序(debugger)、根进程(root process)运行历史、有害应用程序的安装、有害应用程序运行历史、恶意接口、会话伪变造、输入值伪变造及电脑病毒等具备破解威胁能力的要素进行检测时，可以是上述各个要素的检测顺序。

[0077] 而且，关于上述编译级别，如果把动态安全模块的源代码编译(build)成能在上述安全客户端运行的机器语言的话，为了顺利地运行安全管理功能而利用编译器优化地编译。此时，除了代码的optimization level以外，还能创建各式各样的level的代码，相异地实现构成动态安全模块的代码的编译级别而得以创建无数种类的相异动态安全模块。而且，在实现如前所述的源代码的相异的编译级别时，不仅能在创建上述动态安全模块的服务器装置实现，还能在诸如上述用户终端的安全客户端实现。

[0078] 而且，作为一例，执行上述动态安全模块的安全管理的代码的一部分或全部代码的有效期能以选自1小时、3小时、6小时、9小时、12小时、24小时、48小时及72小时所构成的群的时间间隔设定，该有效期截止时，删除上述代码的一部分或全部代码或者禁止使用地配置。因此，如前所述的动态安全模块的有效期截止时，上述安全客户端停止使用动态安全模块，并且接收上述动态安全模块服务器装置所传输的新动态安全模块后进行更新，从而能够有效地防止因动态安全模块被破解或感染病毒而导致上述用户终端发生安全问题的现象。

[0079] 本发明第二实施例的动态安全模块的创建方法是一种以让在用户终端为了安全而执行的代码在每次执行时都不相同的方式创建分配给上述用户终端的动态安全模块的方法，其包括下列步骤：构成上述动态安全模块的代码中可变更的部分的一部分或全部被指定为变量，为上述变量中的至少一个以上分配预设值(S200)；还包括下列步骤：让构成传输到上述用户终端的动态安全模块的代码的一部分或全部代码具备有效期，和上述用户终端的安全客户端创建安全会话(210)；及把上述动态安全模块传输给创建了上述安全会话

的用户终端的安全客户端(220)。

[0080] 亦即,本发明第二实施例的动态安全模块的创建方法使得在用户终端的安全客户端执行安全管理的代码的一部分或全部代码具备预定的有效期地创建动态安全模块,在驱动用户终端时、或在用户终端驱动包含上述安全客户端的应用程序时、或用户终端的用户请求时、或按照上述动态安全模块服务器装置所设定的每一定周期、或按照用户终端所设定的每一定周期等众多情形下和用户终端的安全客户端创建安全会话并且把上述动态安全模块传输给上述用户终端的安全客户端而使得上述动态安全模块经常更新,能够有效地防止因安全模块被破解或感染病毒而导致加载到用户终端的应用程序发生安全问题的现象。

[0081] 而且,上述创建方法以下列步骤执行:从传输到上述安全客户端的动态安全模块接收安全管理结果(230);确认所收到的上述安全管理结果而确认是否发生了安全问题(240);及用户终端没有发生安全问题时,把表示没有发生安全问题的安全管理确认结果值传输给上述安全客户端的动态安全模块(S250)。

[0082] 在此,执行下列步骤:上述用户终端发生了安全问题时,把表示发生了安全问题的安全管理确认结果值传输给上述安全客户端的动态安全模块(S251)。

[0083] 而且,还能执行下列步骤:上述用户终端发生了安全问题时,把命令上述用户终端的应用程序停止的停止指令传输给上述安全客户端的动态安全模块(S252)。

[0084] 亦即,本发明的动态安全模块的创建方法从传输到用户终端的安全客户端的动态安全模块接收安全管理结果并且予以确认,把安全管理确认结果值重新传输给动态安全模块,从而让动态安全模块能在上述用户终端发生安全问题时迅速有效地采取对策。

[0085] 为此,从传输到上述安全客户端的动态安全模块接收作为上述安全管理的安全管理结果并且确认所收到的上述安全管理结果,上述用户终端发生了安全问题时,把命令上述用户终端的应用程序停止的停止指令传输给上述安全客户端的动态安全模块,废弃和上述安全客户端的安全会话,因此能从根本上防止黑客破解动态安全模块后导致用户终端的各种应用程序发生安全问题的现象。

[0086] 亦即,上述用户终端发生安全问题时让加载到上述用户终端的应用程序的驱动迅速停止,从而防止上述应用程序的驱动导致加载到上述用户终端的其它应用程序进一步发生安全问题,废弃上述安全会话而得以迅速阻止黑客对动态安全模块或动态安全模块服务器装置的追踪及分析。

[0087] 在此,安全管理是一种包含着上述动态安全模块为了上述用户终端的安全而执行的全盘管理的概念,其可以举例如下:上述动态安全模块检测是否存在着对包含上述安全客户端的应用程序可能构成破解威胁的要素;针对安装了上述应用程序的终端机的O/S伪变造、应用程序(App)的伪变造、获取最高权限(Rooting)、调试程序(debugger)、根进程(root process)运行历史、有害应用程序的安装、有害应用程序运行历史、恶意接口、会话伪变造、输入值伪变造及电脑病毒等具备破解威胁能力的要素进行检测;把构成上述破解威胁的要素的信息传输给上述动态安全模块服务器装置;治疗针对上述应用程序的病毒;为了防止对于上述应用程序的破解威胁及病毒感染问题而向上述应用程序传输停止指令;上述动态安全模块的有效期截止或黑客破解、病毒感染之类的问题导致动态安全模块停止本身功能。

[0088] 而且，作为一例，收自上述用户终端的安全管理事件可以是用于对上述安全客户端所传输过来的动态安全模块判断其相关参数的详细信息、针对动态安全模块被驱动的状态的状态(state)详细信息、告知发生过破解威胁的安全管理结果信息、以及对于加载到上述用户终端的应用程序的病毒治疗详细信息之类的各式各样事件。

[0089] 而且，上述安全管理结果是上述动态安全模块在上述安全客户端实际执行的安全管理的详细信息，是执行了上述动态安全模块所含具体安全管理功能后的结果值，也是安全管理事件的一部分。例如，可以是对于可构成上述破解威胁的要素存在与否的侦测结果、可构成上述破解威胁的要素的检测结果、对于上述应用程序的病毒治疗及对于可构成破解威胁的要素的清除结果之类的详细信息。

[0090] 而且，上述安全管理确认结果值是上述动态安全模块服务器装置收到上述安全管理结果后以上述安全管理结果为基础分析的对于上述用户终端是否发生安全问题的判断结果。亦即，可以是对于上述用户终端目前是否存在着可构成破解威胁的要素的判断结果、对于加载到用户终端的应用程序是否被破解的判断结果、以及对于上述应用程序是否被病毒或恶意代码感染的判断结果。

[0091] 上述动态安全模块的创建方法创建作为安全会话标识符的会话ID并加以存储，把上述会话ID传输给上述安全客户端使得上述安全客户端存储上述会话ID而得以创建安全会话。利用该会话ID创建安全会话的方法则创建多个安全会话后经常更新安全会话，因此能够提高上述动态安全模块对上述用户终端的安全管理的可靠性与便利性。

[0092] 在此，关于上述安全会话的创建，能以和认证完毕的用户终端的安全客户端创建的方式实现。亦即，为了让上述安全会话的创建进一步提高用户终端的安全性，能够对用户终端的安全客户端进一步进行认证过程以便传输动态安全模块。

[0093] 而且，作为一例，上述用户终端的安全客户端的认证能以下列方式完成：作为包含上述安全客户端的应用程序的应用程序(application)被安装到上述用户终端的同时完成认证、或者上述应用程序被安装到上述用户终端后第一次驱动时完成认证、或者对上述应用程序登录(log in)及注销(log out)时完成认证、或者上述应用程序被安装到上述用户终端后用户通过上述应用程序请求而完成认证。

[0094] 上述创建方法还包括下列步骤：在维持着上述安全会话的期间把关于传输到上述安全客户端的各个上述动态安全模块的参数加以存储。

[0095] 在此，关于动态安全模块的参数是对下列事项的具体信息，该事项为执行传输到上述安全客户端的安全管理的动态安全模块的用于执行安全管理的代码的函数名、指定拟运行的算法的变量、协议字段、指定协议序列的变量、指定编译级别的变量及指定执行代码混淆方法的变量等，是用来把经常更新而具备相异配置的各个动态安全模块予以区分的，其为上述动态安全模块服务器装置决定的信息，也是执行上述动态安全模块的安全管理的代码运行时的信息。

[0096] 而且，上述处理器接收对于传输到上述安全客户端的动态安全模块的详细信息并且验证其是否和上述所存储的动态安全模块的参数的配置相同。对于该动态安全模块的参数变更内容的验证可以如下进行。例如，如果各个参数像A-B-C-D一样地依次传输的动态安全模块的参数在和上述安全客户端所传输过来的详细信息比较时发现不相同并且已变更成不同内容的话，可以推测发生了黑客试图破解之类的情形，可以对此采取措施。

[0097] 图3示出了显示本发明的动态安全模块创建装置的概略配置的模式图。

[0098] 请参阅图3，本发明的动态安全模块创建装置310是一种以让在用户终端350为了安全而执行的代码在每次执行时都不相同的方式创建分配给上述用户终端350的动态安全模块318的装置，其包括：通信单元，通过网络收发安全管理事件312；及处理器314，控制上述通信单元312；上述处理器314让构成上述构成动态安全模块318的代码中可变更的部分的一部分或全部被指定为变量，为上述变量中至少一个以上分配预设值，让构成传输到上述用户终端350的动态安全模块318的代码的一部分或全部代码具备有效期。

[0099] 亦即，本发明的动态安全模块创建装置310由处理器314把在用户终端350的安全客户端352执行安全管理的代码的一部分或全部代码具备预定的有效期的动态安全模块318加以存储或者每次传输时创建，在驱动用户终端350时、或在用户终端350驱动包含上述安全客户端352的应用程序的驱动时、或用户终端350的用户请求时、或按照上述动态安全模块服务器装置310所设定的每一定周期、或按照用户终端350所设定的每一定周期等众多情形下和用户终端350的安全客户端352创建安全会话并且把上述动态安全模块318传输给上述用户终端350的安全客户端352而使得上述动态安全模块318经常更新，能够有效地防止因安全模块被破解或感染病毒等原因而导致加载到用户终端的应用程序发生安全问题的现象。

[0100] 作为一例，上述动态安全模块的可变更部分可以是能够把从代码的函数名、指定拟运行的算法的变量、协议字段、指定协议序列的变量、指定编译级别的变量及指定执行代码混淆方法的变量所构成的群选择的1种以上的要素予以变更的代码。

[0101] 亦即，对于构成在上述用户终端安全客户端为了安全管理而驱动的动态安全模块的代码中像实现驱动起始点的代码一样即使动态安全模块从新更新也不会跟着改变而固定的代码以外的其余可变更的代码，把从代码的函数名、指定拟运行的算法的变量、协议字段、指定协议序列的变量、指定编译级别的变量及指定执行代码混淆方法的变量所构成的群选择的1种以上的要素予以变更而得以创建无数种类的动态安全模块。

[0102] 作为一例，收自上述用户终端350的安全管理事件可以是用于对上述安全客户端352所传输的动态安全模块318判断其相关参数的详细信息、针对动态安全模块318被驱动的状态的状态(state)详细信息、告知发生过破解威胁的安全管理结果信息、以及对于加载到上述用户终端150的应用程序的病毒治疗详细信息之类的各式各样事件。

[0103] 而且，上述用户终端350可以是诸如智能手机、平板电脑、桌上型电脑、笔记本电脑等需要保护安全的各种终端机。

[0104] 上述处理器314从传输到上述安全客户端152的动态安全模块318接收安全管理结果并且确认所收到的上述安全管理结果，把安全管理确认结果值传输给上述安全客户端352的动态安全模块318

[0105] 具体地说，从传输到上述安全客户端352的动态安全模块318接收作为上述安全管理的安全管理结果并且确认所收到的上述安全管理结果，上述用户终端350没有发生安全问题时，把表示没有发生安全问题的安全诊断确认结果值传输给上述安全客户端352的动态安全模块318。

[0106] 而且，而从传输到上述安全客户端352的动态安全模块318接收作为上述安全管理的安全管理结果并且确认所收到的上述安全管理结果，上述用户终端350发生了安全问题

时，把表示发生了安全问题的安全管理确认结果值传输给上述安全客户端352的动态安全模块318。

[0107] 亦即，本发明的动态安全模块创建装置310从传输到用户终端350的安全客户端352的动态安全模块318接收安全管理结果并且予以确认，把安全管理确认结果值重新传输给动态安全模块318，从而让动态安全模块318能在上述用户终端150发生安全问题时迅速有效地采取对策。

[0108] 为此，上述处理器314从传输到上述安全客户端352的动态安全模块318接收作为上述安全管理的安全管理结果并且确认所收到的上述安全管理结果，上述用户终端发生了安全问题时，把把命令上述用户终端350的应用程序停止的停止指令传输给上述安全客户端352的动态安全模块118并且废弃和上述安全客户端352的安全会话，因此能从根本上防止黑客破解动态安全模块318后导致用户终端350的各种应用程序发生安全问题的现象。

[0109] 另一方面，上述处理器314创建作为安全会话标识符的会话ID316并加以存储，把上述会话ID316传输给上述安全客户端352而让上述安全客户端352存储上述会话ID316，从而得以创建安全会话。利用该会话ID创建安全会话的方法则创建多个安全会话后经常更新安全会话，因此能够提高上述动态安全模块318对上述用户终端350的安全管理的可靠性与便利性。

[0110] 上述有效期可以是一种上述有效期截止时删除上述代码的一部分或全部代码或者禁止使用上述代码的一部分或全部代码的有效期。亦即，在上述用户终端350的安全客户端352执行安全管理的代码的一部分或全部代码具备有效期的上述动态安全模块318可以在有效期截止时删除代码的一部分或全部代码，或者为了不执行安全管理而停止使用动态安全模块本身。

[0111] 因此，该动态安全模块318的有效期截止时，上述安全客户端352更新构成动态安全模块318的代码的一部分或全部代码而能够从源头上防止因动态安全模块318被破解或感染病毒而导致发生安全问题的现象。

[0112] 而且，上述处理器314在维持着上述安全会话的期间把关于传输到上述安全客户端352的各个上述动态安全模块318的参数加以存储。

[0113] 在此，关于动态安全模块318的参数是对下述事项的具体信息，该事项为传输到上述安全客户端352执行安全管理的动态安全模块的用于执行安全管理的代码的函数结构、算法的种类、编译级别等，是用来把经常更新而具备相异配置的各个动态安全模块予以区分的，其为在上述动态安全模块服务器装置310决定的信息，因此安全客户端的代码的一部分或全部也会变更。

[0114] 而且，上述处理器314接收关于传输到上述安全客户端352的动态安全模块318的详细信息并且验证其是否和上述所存储的动态安全模块318的参数的配置相同。该动态安全模块的参数变更内容的验证可以如下进行。例如，如果各个参数像A-B-C-D一样地依次传输的动态安全模块的参数在和上述安全客户端352所传输的详细信息比较时发现不相同并且已变更成不同内容的话，可以推测发生了黑客试图破解之类的情形，可以对此采取措施。

[0115] 上述动态安全模块创建装置310还能包括存储器313，该存储器313存储拟传输给上述用户终端350的安全客户端352的动态安全模块318、作为安全会话标识符的会话ID316及关于动态安全模块的参数。

[0116] 亦即，上述动态安全模块服务器装置310把动态安全模块318、会话ID316存储到上述存储器313而得以把上述动态安全模块318与会话ID316顺畅稳定地传输给上述安全客户端352。而且，上述存储器313把关于传输给上述安全客户端352的动态安全模块的参数加以存储，从而能够更稳定地针对关于传输给上述安全客户端352的动态安全模块318的收信内容进行同一性验证。

[0117] 图4示出了显示本发明的一个实施例的动态安全模块创建方法中由相异的函数构成的动态源代码创建例的模式图，图5示出了显示本发明的一个实施例的动态安全模块创建方法中由相异的算法构成的动态算法创建例的模式图，图6示出了显示本发明的一个实施例的动态安全模块创建方法中具备相异的编译级别的动态编译参数创建例的模式图。

[0118] 请参阅这些附图，本发明的动态安全模块创建方法及创建装置在创建动态安全模块时，可以利用从认证安全客户端时收到的用户终端的IP地址(Internet Protocol address)、手机号码、随机数创建器所创建的值所构成的群选择的变量创建各式各样形态的相异动态安全模块。

[0119] 首先，如同图4的动态源代码创建例(图4的下部)一样地，本发明动态安全模块创建方法的动态安全模块可以由下述源代码实现用来在安全客户端创建安全诊断执行结果的逻辑，该源代码由每次创建时改变的相异函数所构成。

[0120] 如同图4的创建例(图4的上部)一样地，现有的一般源代码在分析源代码时会直接泄露出相应于源代码的具体函数名，因此黑客很容易掌握由该源代码构成的主逻辑。但如同图4的创建例(图4的下部)一样地，本发明的动态安全模块由于构成主逻辑的源代码的函数没有确定而是由以概率(%)方式表现的动态源代码实现的，该动态源代码概率(%)则是随机字符串所构成的源代码被采纳的概率(%)，从而使得黑客无法轻易掌握动态安全模块的主逻辑。作为一例，该动态源代码可以使用模板框架(Template framework)轻易实现。

[0121] 而且，如同图5的动态安全模块的动态算法创建例一样地，作为一例，本发明的动态安全模块以3种相异算法实现执行同一安全管理功能的逻辑并且让这些算法中的一个算法被选定为用于执行安全管理的算法，使得黑客每次都需要进行不同的算法分析而显著地提高了破解动态安全模块本身的难度。

[0122] 而且，如同图6的动态编译参数的创建例一样地，本发明的动态安全模块在动态安全模块的编译(build)过程中以除了optimization level编译结果物以外的各式各样level的编译结果物创建，因此每次都能让所创建的各个动态安全模块的代码配置不同地实现。

[0123] 图7示出了显示本发明的一个实施例的动态安全模块创建方法中会话ID及动态安全模块参数创建例的模式图，图8示出了显示本发明的一个实施例的动态安全模块创建方法中动态安全模块协议字段创建例的模式图，图9示出了显示本发明的一个实施例的动态安全模块创建方法中动态安全模块协议序列创建例的模式图。

[0124] 请参阅这些附图，本发明的动态安全模块创建方法在创建安全会话时，如同图7的会话ID及动态安全模块参数创建例一样地，创建作为安全会话标识符的会话ID并且存储到服务器装置的处理器，把上述会话ID传输给上述安全客户端而让上述安全客户端存储上述会话ID，从而能够创建安全会话。而且，可以把在维持着上述安全会话的期间创建的上述关于动态安全模块的参数加以存储。

[0125] 亦即，如图7所示，作为一例，上述动态安全模块创建方法在上述动态安全模块服务器装置与用户终端的安全客户端创建11836381的会话ID地创建了安全会话时，对于上述安全客户端所传输过来的动态安全模块的详细信息验证其参数(param)为A、B、C而这时候的状态(state)为1、2；创建72365784的会话ID地创建安全会话时，对于安全客户端所传输的动态安全模块的详细信息验证其参数(param)为C、B、A而这时候的状态(state)为0、3；创建87656501的会话ID地创建了安全会话时，对于安全客户端所传输的动态安全模块的详细信息验证其参数(param)为B、A、C而这时候的状态(state)为3、2。在此，该参数与状态详细信息可以是收自上述用户终端的安全管理事件。

[0126] 而且，也可以让各安全会话各自不同地设定上述各个安全会话的变更时间间隔、各安全会话各自的动态安全模块的传输时间间隔，使得黑客更难分析动态安全模块。

[0127] 而且，如同图8的动态安全模块协议字段创建例一样地，本发明的动态安全模块创建方法可以让和安全客户端之间的协议字段(brown、white、black)在每一个各自创建的动态安全模块给予不同设定后传输给用户终端的安全客户端。

[0128] 如前所述地，传输到安全客户端的动态安全模块的协议字段每次不同的话，黑客需要针对每次都不同的协议字段全部进行分析，使得黑客更难破解动态安全模块。

[0129] 而且，如同图9的动态安全模块协议序列创建例一样地，本发明的动态安全模块创建系统可以让在安全客户端运行的动态安全模块的协议序列(A->B->C->D)在每一个各自创建的动态安全模块诸如A->D->B->C、D->C->B->A、B->A->D->C一样地给予不同设定后传输给安全客户端，因此让执行安全管理的具体功能的驱动顺序每次都不一样地配置而得以构成更难破解的动态安全模块。

[0130] 本发明的动态安全模块创建装置110包括处理器314、通信单元312及存储器313。

[0131] 上述处理器314创建控制信号并且可以控制包括通信单元312与存储器313在内的上述创建装置310。在此，通信单元312可以利用各种协议和外部装置进行通信而收发数据，以有线或无线方式接入外部网络后收发内容、应用程序之类的数字数据。

[0132] 而且，上述存储器313是一种能够存储包括音频、照片、视频、应用程序等在内的各式各样数字数据的装置，其意味着闪存，RAM(Random Access Memory)、SSD(Solid State Drive)之类的各式各样数字数据存储空间。该存储器113可以临时存储通过通信单元312从外部装置接收的数据。

[0133] 本发明的动态安全模块的创建方法以能够通过各式各样的电脑装置执行的程序指令形态实现而得以记录在计算机可读存储介质。上述计算机可读存储介质能以单独或组合方式包含程序指令、数据文件、数据结构等。记录在上述介质的程序指令可以是专门为本发明设计地组成者，也可以是电脑软件的本领域人士所熟知并且可使用者。

[0134] 前文利用具体构成要素之类的特定事项和有限的实施例及附图说明了本发明，但这些内容仅仅是为了帮助全盘了解本发明而提供的，不得因此把本发明限定于上述实施例，本技术领域中具有通常知识者能从该记载内容进行各种修改及变形。

[0135] 因此本发明的思想不能局限于前面说明的实施例，本发明的思想范畴应该包括权利要求书及等价于该权利要求书或者等值变形者全部。

[0136] 工业应用可能性

[0137] 本发明揭示了一种动态安全模块的创建方法及创建装置，该方法以让在用户终端

为了安全而执行的代码在每次执行时都不相同的方式创建分配给上述用户终端的动态安全模块，其包括下列步骤：构成上述动态安全模块的代码中可变更的部分的一部分或全部被指定为变量，为上述变量中的至少一个以上分配预设值；构成传输到上述用户终端的动态安全模块的代码的一部分或全部代码具备有效期。

[0138] 根据本发明，把执行安全管理的源代码的一部分或全部代码具备预定的有效期的动态安全模块传输给用户终端的安全客户端，让针对用户终端的各种应用程序的安全模块随时更新，因此让针对上述应用程序的破解变得困难而得以显著地提高用户终端的安全性(security)。

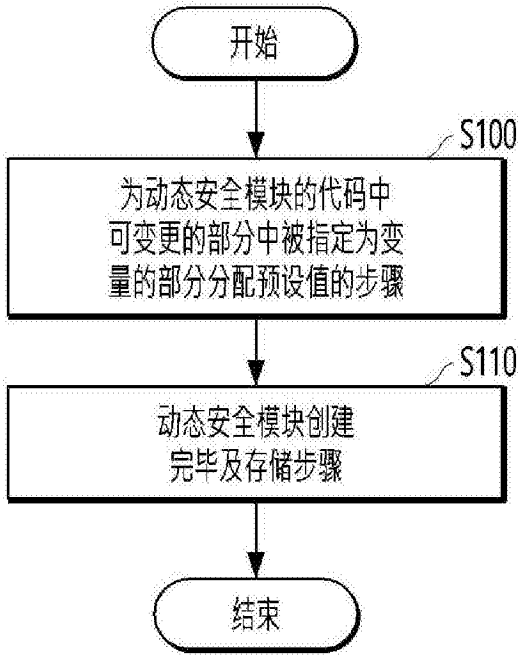

开始
S100
为动态安全模块的代码中可变更的部分中被指定为变量的部分分配预设值的步骤
S110
动态安全模块创建完毕及存储步骤
结束

图1

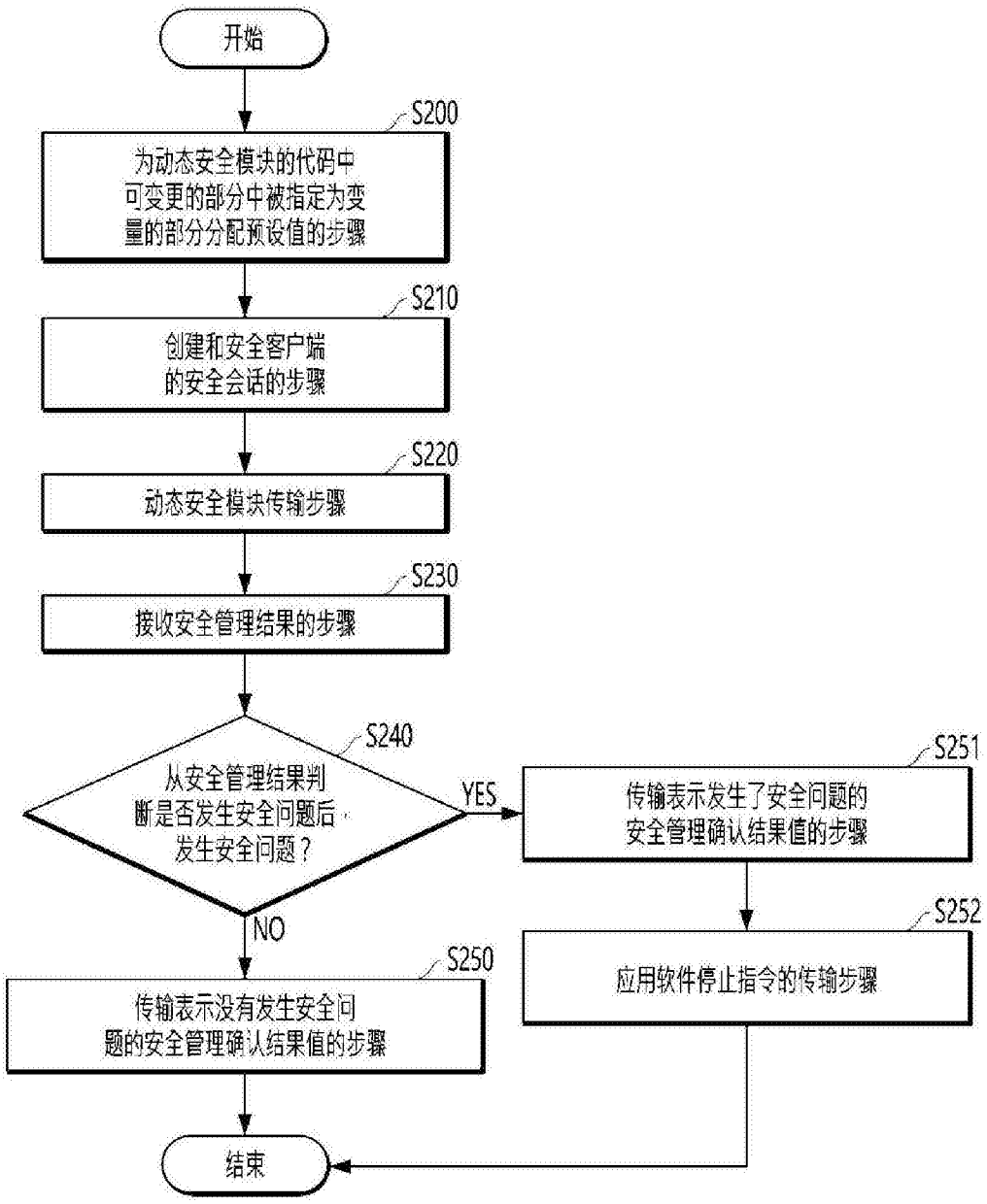

开始
S200
为动态安全模块的代码中可变更的部分中被指定为变量的部分分配预设值的步骤
S210
创建和安全客户端的安全会话的步骤
S220
动态安全模块传输步骤
S230
接收安全管理结果的步骤
S240
从安全管理结果判断是否发生安全问题后，发生安全问题？
YES
NO
S251
传输表示发生了安全问题的安全管理确认结果值的步骤
S252
应用软件停止指令的传输步骤
S250
传输表示没有发生安全问题的安全管理确认结果值的步骤
结束

图2

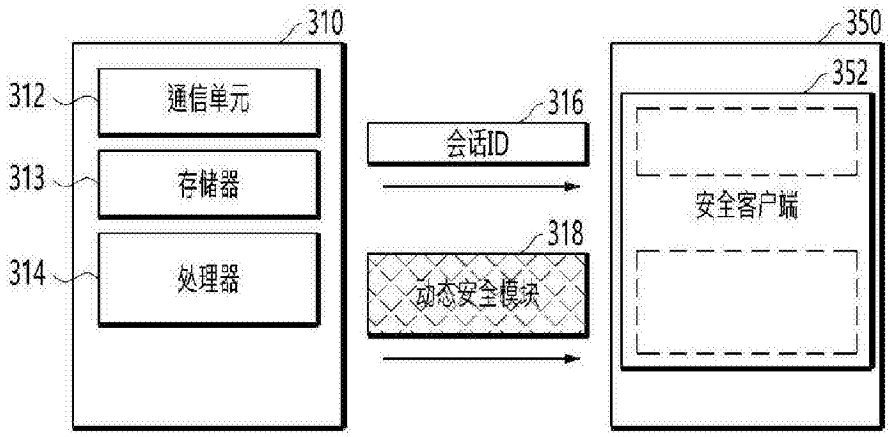


图3

```
int two_times(x) {
  return 2*x;
}

int three_more(x) {
  return x + 3;
}

int result(x) {
  return two_times(x) * three_more(x);
}
```

```
int <%=TWO_TIMES%>(x) {
  return 2*x;
}

int <%=THREE_MORE%>(x) {
  return x + 3;
}

int result(x) {
  return <%=TWO_TIMES%>(x) * <%=THREE_MORE%>(x);
}
```

```
TWO_TIMES=随机字符串
THREE_MORE=随机字符串
```

图4

```
<%
case SUM_ALGORIGTHM_IDX
when 0
%>
int sum(a) {
  int i, s = 0;
  for (i = 1; i <= a; i++)
    s += i;
  return s;
}
<%
when 1
%>
int sum(a) {
  int s = 0;
  while (a > 0)
    s += a--;
  return s;
}
<%
when 2
%>
int sum(a) {
  if (a == 0)
    return 0;
  return a + sum(a - 1);
}
<%
end
%>
```

```
SUM_ALGORIGTHM_IDX=rand(3)
```

图5

```
CFLAGS=-g -O<%=OPTIMIZATION_LEVEL%>
```

```
OPTIMIZATION_LEVEL=['0', '1', '2', 's'].sample
```

图6

会话_id	参数1	参数2	参数3	状态1	状态2
11836381	A	B	C	1	2
72365784	C	B	A	0	3
87656501	B	A	C	3	2

图7

pants: brown shirts: white hat: black

aaa: brown bbb: white ccc: black	hat: brown paants: white haat: black	KV3gLmDj: brown uSqU3cdK: white 7/wETz94: black

图8

A -> B -> C -> D

A -> D -> B -> C	D -> C -> B -> A	B -> A -> D -> C

图9