

一种基于装置代码的风险扫描方法、系统和运算装置

技术领域

本发明涉及代码风险防控领域，尤其涉及一种基于装置代码的风险扫描方法、系统和运算装置。

背景技术

针对在线服务器（例如：网站服务器）上的网站后端系统和在线运行的硬件装置进行漏洞检测时。由于服务器上的中间码、二进制代码，以及硬件装置里的二进制代码皆是人类无法识别的代码（例如：Linux Kernel、Web Server 等），且该服务器和硬件装置已经在线运行，因此目前的现有技术是经由网络，依据一特定漏洞的行为描述，对该服务器和硬件装置发出仿真攻击的一网络封包，在该服务器和硬件装置收到该网络封包后，监测该服务器和硬件装置的反应是否符合该特定漏洞的行为描述，若是相符，即表示该在线运行的服务器和硬件装置中存有该特定漏洞，进而为服务器和在线硬件装置的运营者提供漏洞扫描的功效。

针对在线服务器及/或硬件装置的漏洞进行分析和风险的扫描时，由于运行于服务器及/或硬件装置中的代码是以中间码或二进制代码为主，在缺乏源代码的情况下，无法以补丁的源代码来跟在线系统的源代码进行比对；源代码的比对，在没有源代码的情况下将无法实施。而仿真封包的漏洞分析，则需网络环境的支持，在脱机或者是网络不能正常运作的情况下，模拟封包无法送到待测的在线的服务器及/或硬件装置，仿真封包的漏洞分析和风险监控亦无法实施。且当特定漏洞的驱动并非是能够以模拟封包来触发，则该特定漏洞亦无法以模拟封包的方式来检测。

针对物联网感测器、网路通讯设备（例如：WiFi 无线路由器）或者是其他运算能力有限的嵌入式装置，代码的成份分析并无法像个人电脑上的病毒扫描软件一样，直接提供在该等装置里进行运算，一方面个人电脑的软硬件规格之设计，除了考虑到操作系统本身所需的算力外，亦会保留出足够的算力供用户所安装的应用程序所使用，另一方面个人电脑所提供的是通用型的作业平台，并不针对单一或特定功能所使用，使得不同的应用程序得以透过安装的方式，扩充至作业环境中使用；因此，个人电脑的病毒扫描软件得以安装在个人电脑上使用。对于物联网感测器、网路通讯设备（例如：WiFi 无线路由器）或者是其他运算能力有限的嵌入式装置而言，一方面其功用并不是作为通用型的作业平台，而是提供单一或特定服务的装置，不具备随意安装应用程序来扩充其工作能力的条件，另一方面在软硬件规格的设计上，是以最佳化其所提供的单一或特定的服务为主；因此，代码成份分析难以在该等设备或装置中运行。

综合以上的说明可知，在信息安全的风险扫描技术领域里，如何对缺乏源代码、在线运行及/或是软硬件规格针对单一或特定功能设计的硬件装置进行漏洞扫描是一重要的技术课题。目前尚未有一种装置代码风险扫描方法、软件系统和运算装置，能够在缺乏装置系统的源代码、网络脱机、算力不足及/或是无法扩充应用程序的状态，为装置提供漏洞分析的风险扫描方法与运用该方法的系统，故仍亟待开发。

发明内容

针对上述技术问题，本发明提供一种基于装置代码的风险扫描方法、系统和运算装置，通过自生成的更新记录自动向用户发送扫描结果，提高了风险扫描的效率与准确性。

方案一：

一种基于装置代码的风险扫描方法，包括：

获取一装置代码，所述装置代码是从第一装置所获取，并将所述装置代码自第一装置发送至第二装置；其中，所述装置代码包括至少一软件代码；

生成一更新记录；其中，所述更新记录中包括所述装置代码与所述第一装置及/或所述第二装置之间的关系记录；

当检测到所述装置代码中存在安全风险时，根据所述更新记录向所述第一装置及/或所述第二装置发出扫描结果。

进一步的，所述发出扫描结果，是指透过至少一网路通信渠道，向所述第一装置和第二装置的用户、运营者或管理者中至少一人，发出一扫描结果的通知。

进一步的，所述至少一软件代码包含至少一二进制代码。

进一步的，所述获取装置代码，具体包括：

依据一更新请求，从所述第一装置的一存储媒体中获取所述装置代码。

进一步的，所述获取装置代码的方法还包括：

当获取所述更新请求时，根据所述更新请求中的一版本信息或一装置规格信息，在所述存储媒体中获取与所述版本信息或所述装置规格信息对应的装置代码，作为所述装置代码；其中，所述装置规格信息包括一装置的产品规格、硬体规格以及软韧体规格中至少一个。

进一步的，所述将所述装置代码发送至第二装置，具体包括：

根据所述更新请求所包括的第二装置的网络位置信息，将所述装置代码发送至所述第二装置。

进一步的，所述检测到所述装置代码中存在安全风险，具体包括：

当至少一代码分析事件触发时，将至少一风险代码与所述至少一软件代码进行成份内容的比对；其中，所述至少一风险代码包括与所述至少一软件代码关联的补丁代码、恶意程序代码以及任意一种由计算机程序语言编写的计算机程序代码中的至少一个。

进一步的，所述至少一风险代码是依据至少一风险代码登录列表而被预先搜集，或者是在一风险代码被新增或更新至所述至少一风险代码登录列表时所搜集。

进一步的，所述至少一代码分析事件是在包括取得所述至少一软件代码的一组成清单时所触发，或者是所述至少一风险代码被新增或被更新时所触发。

进一步的，所述将所述至少一风险代码与所述至少一软件代码进行比对，具体包括：

 撷取相对应于所述至少一风险代码的至少一第一成份特征；

 撷取相对应于所述至少一软件代码的至少一第二成份特征；

 比对所述至少一第一成份特征和所述至少一第二成份特征。

进一步的，所述至少一第一成份特征是藉由对相对应于所述至少一风险代码的代码组成内容及/或代码执行结果进行剖析后所得。

进一步的，所述代码组成内容包括所述至少一风险代码及/或所述至少一风险代码编译后的至少一第一中间代码，所述代码执行结果则包括对所述至少一风险代码及/或所述至少一第一中间代码做模拟执行时，所述至少一风险代码及/或所述至少一第一中间代码在模拟执行过程中所显露出的语义信息。

进一步的，所述至少一第二成份特征是藉由对相对应于所述至少一软件代码的至少一代码组成内容及/或至少一代码执行结果进行剖析后所得。

进一步的，所述至少一代码组成内容包括至少一二进制代码及/或所述至少一二进制代码反组译后的至少一第二中间代码，所述至少一代码执行结果则包括对所述至少一二进制代码及/或所述至少一第二中间代码做模拟执行时，所述至少一二进制代码及/或所述至少一第二中间代码在模拟执行过程中所显露出的语义信息。

进一步的，所述中间代码的程序语言结构是由一中间语言、一中间表示、

一结构化语言，及/或一结构化协议所宣告而成。

进一步的，所述代码分析事件触发前，还包括：

依据所述至少一软件代码的组成清单，对至少一代码分析事件进行侦测，相对应于所述至少一风险代码的所述代码分析事件是所述至少一代码分析事件的其中之一。

进一步的，所述组成清单是在所述装置代码被获取时，对所述装置代码的成份组成进行扫描及/或剖析后所取得。

进一步的，所述组成清单包括所述装置代码本身的元数据及/或所述装置代码成份组成中所含的所述至少一软件代码的元数据。

进一步的，所述至少一软件代码是以包括系统核心、驱动程序、应用程序、组件，及/或类别库的型态存在于所述装置代码的成份组成中。

进一步的，依据所述组成清单，对所述组成清单中所含各个软件代码所相对应的风险代码登录列表进行监控，藉由监控所述风险代码登录列表的异动来侦测代码分析事件。

进一步的，所述组成清单的获取方法具体包括：

所述装置代码是一系统映像档，对系统映像档中所含的成份组成进行扫描及/或剖析，辨识出存在于所述系统映像档中的所述至少一软件代码，进而得到所述至少一软件代码的所述组成清单；

或者所述装置代码是一软件代码包裹，对所述软件代码包裹中所含的成份组成进行扫描及/或剖析，辨识出存在于所述软件代码包裹中的所述至少一软件代码，进而得到所述至少一软件代码的所述组成清单。

进一步的，所述根据所述更新记录向所述第一装置及/或所述第二装置发出扫描结果，具体包括：

对所述更新记录进行查找，获取所述更新记录中的关系记录；

根据所述关系记录对所述第一装置和所述第二装置的用户、运营者或管理者的至少一个发出扫描结果。

进一步的，所述扫描结果包括扫描报告与扫描状态通知信息中至少一个；其中，所述扫描报告用于展示所述至少一软件代码与所述至少一风险代码的成份内容比对结果；所述扫描状态通知信息用于对所述第一装置和所述第二装置的用户、运营者或管理者中的至少一个提供扫描状态的通知。

方案二：

一种基于装置代码的风险扫描系统，包括：代码发送模块、更新记录生成模块以及扫描结果通知模块；

所述代码发送模块用于获取一装置代码，所述装置代码是从第一装置所获取，并将所述装置代码自第一装置发送至第二装置；其中，所述装置代码包括至少一个软件代码；

所述更新记录生成模块用于生成一更新记录；其中，所述更新记录中包括所述装置代码与所述第一装置及/或所述第二装置之间的关系记录；

所述扫描结果通知模块用于当检测到所述装置代码中存在安全风险时，根据所述更新记录向所述第一装置及/或所述第二装置发出扫描结果。

进一步的，还包括：第一特征提取单元、第二特征提取单元和特征比对单元；

所述第一特征提取单元，用于撷取相对应于至少一风险代码的至少一第一成份特征；

所述第二特征提取单元，用于撷取自相对应于所述至少一软件代码的至少一第二成份特征；

所述特征比对单元，用于对至少一第一成份特征和至少一第二成份特征进行比对。

进一步的，所述第一特征提取单元或第二特征提取单元包括至少一剖析单元和至少一撷取单元；

所述至少一剖析单元，用于对相对应于所述至少一风险代码的代码组

成内容及/或代码执行结果进行剖析后得到所述至少一第一成份特征，及/或对相对应于所述至少一软件代码的代码组成内容及/或代码执行结果进行剖析后得到所述至少一第二成份特征；

所述至少一撮取单元，用于撮取剖析后所得到的所述至少一第一成份特征及/或所述至少一第二成份特征。

进一步的，还包括：至少一侦测单元，

所述至少一侦测单元，用于依据所述至少一个软件代码的组成清单，对组成清单中所含各个软件代码所相对应的风险代码登录列表进行监控，藉由监控所述风险代码登录列表的异动来侦测代码分析事件。

方案三：

一种基于装置代码的风险扫描的运算装置，包括：代码发送模块、更新记录生成模块以及扫描结果通知模块；

所述代码发送模块用于获取一装置代码，所述装置代码是从第一装置所获取，并将所述装置代码自第一装置发送至第二装置；其中，所述装置代码包括至少一个软件代码；

所述更新记录生成模块用于生成一更新记录；其中，所述更新记录中包括所述装置代码与所述第一装置及/或所述第二装置之间的关系记录；

所述扫描结果通知模块用于当检测到所述装置代码中存在安全风险时，根据所述更新记录向所述第一装置及/或所述第二装置发出扫描结果。

附图说明

图1是本发明一种基于装置代码的风险扫描方法的流程示意图；

图2是本发明一种基于装置代码的风险扫描系统的结构示意图。

图3是本发明一种基于装置代码的风险扫描运算装置的结构示意图。

图中，1、风险扫描系统；2、代码发送模块；3、更新记录生成模块；

4、扫描结果通知模块；5、第一装置；6、第二装置；11、运算装置；21、代码发送模块；31、更新记录生成模块；41、扫描结果通知模块。

具体实施方式

本发明得藉由以下描述，包括以下的术语汇编以及结论性实例，而更充分地理解。为简洁起见，本说明书中引用之出版物，包括专利的公开内容，系并入本文以供参考。

以下系提出实施例进行详细说明，本发明的实施例是非限制性的，并且仅代表本发明之各种态样及特征，实施例仅用以作为范例说明，并不会限缩本发明欲保护之范围。此外，实施例中之图式系省略不必要或以通常技术即可完成之组件，以清楚显示本发明之技术特点。

就最受限制的技术意义而言，本文所述的「软件代码」的代码组成内容包括任一种供加载和执行用的二进制代码（Binary Code）、中间码，及/或任一种由计算机程序语言编写的计算机程序代码。本文所述的「装置代码」是用于在一装置上运行，并于该装置上为该装置提供逻辑运算及服务的代码，所述装置代码由包括二进制代码、中间码，及/或是任一种由计算机程序语言编写的计算机程序代码所组成，亦即所述装置代码包含至少一软件代码，所述至少一软件代码是以包括系统核心、驱动程序、应用程序、组件，及/或类别库的组件型态存在于所述装置代码的成份组成中。本文所述的「二进制代码」可包括任一种以二进制作作为表示格式的代码。本文所述的「中间代码」可包括任一种以一中间语言、中间表示、结构化语言，及/或结构化协议所宣告的结构所表示的代码；例如，遵循一中间表示所定义的格式而表示的 Java Bytecode，以及从二进制代码反组译而得的 LLVM bitcode，皆为一种中间代码，也可视为中间码。本文所述

的「风险代码」的代码组成内容包括任一种供加载和执行用的二进制代码（Binary Code）、中间码，及/或任一种由计算机程序语言编写的计算机程序代码，所述风险代码的种类包括一补丁代码、恶意程序代码，及/或任一种用于修正或产生一软件漏洞（Vulnerabilities）或软件病毒的代码。本文所述的「元数据」又称诠释数据、中介数据或元数据，是为描述一对象或该对象相关信息之数据。本文所述的「风险代码登录列表」可包括任一种依据一结构化语言及/或结构化协议所宣告的结构所登录、注册及/或表示的一列表，所述列表可以包括一文件、资料库及/或网页的形式储存和发布，所述列表的内容包含本文所述风险代码的登录信息，其中所述登录信息中，包括风险代码本身的内容、风险代码的元数据、风险代码所对应的软件漏洞信息或软件病毒信息；其中 CVE（Common Vulnerabilities and Exposures）列表（CVE Repository）是本文所述风险代码登录列表的一种实施态样，但不以此为限。本文所述的「语义信息」可包括在模拟执行一代码时，在执行过程中从内存及/或中间变量取出的值、执行过程中各指令的执行历程、函数的输出/输入值，及/或任一种可被撷取的数值化信息。两份代码的语义信息的全部或一部份片段，可作为两相比对用的成份特征，依比对的相符程度，决定出两份代码的相似度。

又，本文所述的「代码发送模块」、「更新记录生成模块」、「扫描结果通知模块」、「第一特征提取单元」、「第二特征提取单元」、「特征比对单元」、「剖析单元」、「撷取单元」和「侦测单元」是一种提供逻辑运算或服务的处理单元，所述处理单元的实施态样可包括一类别库、软件组件、软件代理程序、应用程序、任一种可被内建、安装、引入或扩充至本文所述「基于装置代码的风险扫描系统或运算装置」中运行的程序区块，或者是任一种以硬件描述语言所设计而可被嵌入本文所述「基于装

置代码的风险扫描的运算装置」的集成电路单元。

本文所述的「基于装置代码的风险扫描系统」，其实施态样可包括一系统韧体、应用程序、软件引擎、网站系统、操作系统，或者是任一种可被程序扩充的软件平台。于一较佳实施例中，本文所述「基于装置代码的风险扫描系统」可以部署在同一机器上运行，亦即将本文所述代码发送模块、更新记录生成模块、扫描结果通知模块、第一特征提取单元、第二特征提取单元、特征比对单元、剖析单元、撷取单元、侦测单元，全部集成在同一系统中，并将该系统部署至一机器上运行。于另一较佳实施例中，本文所述「基于装置代码的风险扫描系统」可以透过多部机器的协同来加以实施，亦即将本文所述代码发送模块、更新记录生成模块、扫描结果通知模块、第一特征提取单元、第二特征提取单元、特征比对单元、剖析单元、撷取单元、侦测单元等处理单元，提供至不同的机器中，不同机器里的处理单元，彼此之间经由包括 internet、WiFi、蓝牙等联机方式来协同交互，进而通过多部机器来共同集成为一基于装置代码的风险扫描系统。

本文所述的「基于装置代码的风险扫描的运算装置」，其实施态样可包括一网络通讯设备、服务器，或者是任一种具连网、数据处理或控制能力的资通讯设备。于一较佳实施例中，本文所述「基于装置代码的风险扫描的运算装置」可以是单一机器所实施，亦即将本文所述代码发送模块、更新记录生成模块、扫描结果通知模块、第一特征提取单元、第二特征提取单元、特征比对单元、剖析单元、撷取单元、侦测单元，全部集成在同一机器中，作为基于装置代码的风险扫描的运算装置。于另一较佳实施例中，本文所述「基于装置代码的风险扫描的运算装置」可以由多部机器的协同来加以实施，亦即将本文所述代码发送模块、更新记录生成模块、扫描结果通知模块、第一特征提取单元、第二特征提取单元、特征比对单元、

剖析单元、撷取单元、侦测单元等处理单元，提供至不同的机器中，不同机器里的处理单元，彼此之间经可以经由包括 internet、WiFi、蓝牙等联机方式来协同交互，进而通过多部机器来共同集成为一基于装置代码的风险扫描的运算装置。

承上，于一较佳实施例中，本文所述的「代码发送模块」、「更新记录生成模块」、「扫描结果通知模块」、「第一特征提取单元」、「第二特征提取单元」、「特征比对单元」、「剖析单元」、「撷取单元」和「侦测单元」可以个别实作于不同的处理单元中。于另一较佳实施例中，亦可于同一处理单元里，对本文所述的「代码发送模块」、「更新记录生成模块」、「扫描结果通知模块」、「第一特征提取单元」、「第二特征提取单元」、「特征比对单元」、「剖析单元」、「撷取单元」和「侦测单元」中的至少二者提供实作。

下面结合附图和具体实施方式对本发明的内容做进一步详细说明。

参见图 1，为本发明实施例提供的一种基于装置代码的风险扫描方法的流程示意图，具体包括以下步骤：

S1、获取一装置代码，所述装置代码是从第一装置 5 所获取，并将所述装置代码自第一装置 5 发送至第二装置 6；其中，所述装置代码由第一装置 5 生成，且包括至少一个软件代码；

S2、生成一更新记录；其中，所述更新记录中包括所述装置代码与所述第一装置 5 及/或所述第二装置 6 之间的关系记录；

S3、当检测到所述装置代码中存在安全风险时，根据所述更新记录向所述第一装置 5 及/或所述第二装置 6 发出扫描结果。

如图 2 所示为本发明一种装置代码风险扫描系统 1 的结构框图。提供本案装置代码风险扫描方法于一较佳实施例的说明。其中，风险扫描系统 1 是一网站系统，所述网站系统可以部署在第一装置 5、第二装置 6，或者是任一具连网及逻辑运算处理能力的运算装置 11 上；代码发送模块 2、更新记录生成模块 3、扫描结果通知模块 4 是集成至风险扫描系统 1 中的处理单元。

于一较佳实施例中，风险扫描系统 1 部署在第二装置 6，则第一装置 5 得以透过代码发送模块 2 所提供的一应用程序界面（API，Application Programming Interface），本身运行于第一装置 5 的软件系统以呼叫所述应用程序界面的实施方式，将一装置代码提供至代码发送模块 2，让代码发送模块 2 得以获取从第一装置 5 所获取的一装置代码，并令所述装置代码得以自第一装置 5 发送至第二装置 6，所述应用程序界面可以包括 REST API、Web Service 等技术实现，但不以此限。代码发送模块 2 本身的实作也可以包括一网页前端程序或者是以 Java 语言所实现的一软件代理人程序（Software Agent），第一装置 5 得以透过浏览器动态载入以网页前端程序所实现的代码发送模块 2，将所述网页前端程序执行于浏览器上，或者是由风险扫描系统 1 提供用于下载所述软件代理人程序的另一应用程序界面后，由第一装置 5 呼叫所述另一应用程序界面，下载取得所述软件代理人程序，将所述软件代理人程序动态载入并执行于第一装置 5 的 Java 虚拟环境中。完成所述动态载入和执行所述网页前端程序或所述软件代理人程序后，所述网页前端程序或所述软件代理人程序即可在第一装置 5 上获取从第一装置 5 所获取的所述装置代码，并通过所述应用程序界面将所述装置代码自第一装置 5 发送至第二装置 6。所述装置代码是储存于第一装置 5 的存储媒体中的装置代码，所述网页应用程序或所述软件代理人程序可藉由读取所述存储媒体来获取所述的装置代码。另，代码发送模块 2 亦可直接建立 TCP/UDP Socket 连线至第一装置 5，例如可以一授权的身分透过 SSH（Secure Socket Shell）

通讯协定的连线接入第一装置 5，通过存取存储媒体的系统指令遍历存储媒体和寻找装置代码后，透过 SCP(Secure Copy Protocol)通讯协定的连线从第一装置 5 的存储媒体中获取所需的装置代码，将获取的装置代码发送至第二装置 6，令所述装置代码得以自第一装置 5 发送至第二装置 6。

于一较佳实施例中，风险扫描系统 1 部署在第一装置 5，一装置代码是储存于第一装置 5 的存储媒体中的装置代码，代码发送模块 2 藉由读取所述存储媒体来获取所述装置代码，即可建立 TCP/UDP Socket 连线至第二装置 6，通过彼此约定好的通讯协议，将所述装置代码发送至第二装置 6，并更新为第二装置 6 所运行的装置代码。例如：代码发送模块 2 可建立 TCP/UDP Socket 连线至第二装置 6，透过一授权的身分透过 SSH(Secure Socket Shell)通讯协定连线的接入第一装置 6，透过 SCP(Secure Copy Protocol)通讯协定的连线从第一装置 5 的存储媒体中获取所需的装置代码，将获取的装置代码发送至第二装置 6，令所述装置代码得以自第一装置 5 发送至第二装置 6，并更新至第二装置 6，使得所述装置代码成为第二装置 6 所运行的装置代码。

于一较佳实施例中，风险扫描系统 1 部署在有别于第一装置 5 和第二装置 6 以外的一运算装置 11，通过均等于上述“风险扫描系统 1 于第二装置 6”的实施方式，部署于所述运算装置 11 的风险扫描系统 1，得以透过第一装置 5 呼叫代码发送模块 2 的应用程序界面及/或将代码发送模块 2 所包括的网页应用程序或软件代理人程序动态载入于第一装置 5 的方式，令代码发送模块 2 从第一装置 5 获取一装置代码，即可建立一 TCP/UDP Socket 连线至第二装置 6，通过彼此约定好的通讯协议，将所述装置代码发送至第二装置 6。所述装置代码是储存于第一装置 5 的存储媒体中的装置代码。

于一较佳实施例中，第二装置 6 上可以开通一 HTTP 接口，供代码发送模块 2 对所述 HTTP 接口建立一 TCP/UDP Socket 连线，并通过 HTTP 通讯协定将所述装置代码传输至第二装置 6。

上述从第一装置 5 获取装置代码并发送至第二装置 6 的方式，并不以此为限，熟知本技艺人士可依据实际应用需求而进行任何均等的变更设计。通过上述技术实施方式之效益在于，风险扫描系统 1 部署于第二装置 6 时，无论第一装置 5 是一在线服务器、物联网感测器、网路通讯设备（例如：WiFi 无线路由器）或者是其他运算能力有限的嵌入式装置，对从第一装置 5 所获取的装置代码的代码成份分析之运算工作，皆不需要在第一装置 5 上执行；亦不需要在第一装置 5 上安装额外的应用程序以获取所述的装置代码。同样地，风险扫描系统 1 部署于第一装置 5 时，无论第二装置 6 是一在线服务器、物联网感测器、网路通讯设备（例如：WiFi 无线路由器）或者是其他运算能力有限的嵌入式装置，对运行于第二装置 6 上的装置代码的代码成份分析之运算工作，皆不需要在第二装置 6 上执行。而在风险扫描系统 1 部署于有别于第一装置 5 和第二装置 6 的另一运算装置 11 时，无论第一装置 5 及/或第二装置 6 是一在线服务器、物联网感测器、网路通讯设备（例如：WiFi 无线路由器）或者是其他运算能力有限的嵌入式装置，对从第一装置 5 所获取的装置代码的代码成份分析之运算工作，及/或是对运行于第二装置 6 上的装置代码的代码成份分析之运算工作，皆不需要在第一装置 5 和第二装置 6 上执行。

于一较佳实施例中，风险扫描系统 1 中的代码发送模块 2 是因应一更新请求而从第一装置 5 获取一装置代码。

于一较佳实施例中，风险扫描系统 1 是在第二装置 6 运行，所述更新请

求是在第一装置 5 上生成的更新请求，于生成该更新请求时，一版本信息或一装置规格信息被提供至所述更新请求中。方案一，所述更新请求由本身运行于第一装置 5 上的软件系统所生成，于生成该更新请求时，一版本信息或一装置规格信息被提供至所述更新请求中，所述软件系统根据所述更新请求中的所述版本信息或所述装置规格信息，在第一装置 5 的存储媒体中获取与所述版本信息或所述装置规格信息对应的一装置代码后，由所述软件系统呼叫代码发送模块 2 所提供的应用程序界面，将所述装置代码提供至代码发送模块 2，或者是由所述软件系统呼叫风险扫描系统 1 所提供的用于提交更新请求的一应用程序界面将所述更新请求提交予风险扫描系统 1 的代码发送模块 2 后，由第二装置 6 上的代码发送模块 2 透过一授权的身分，以 SSH (Secure Socket Shell) 通讯协定的连线接入第一装置 5，根据所述更新请求中的所述版本信息或所述装置规格信息，以通过存取存储媒体的系统指令遍历存储媒体来找出装置代码后，透过 SCP (Secure Copy Protocol) 通讯协定的连线从第一装置 5 的存储媒体中获取所需的装置代码。方案二，所述更新请求是在一用户在动态载入执行于第一装置 5 上的网页前端程序或软件代理人程序的人机界面上进行操作（例如：对用于建立和提交更新请求的界面进行操作）而生成，于生成该更新请求时，所述用户可以将一版本信息或一装置规格信息藉由所述人机界面而输入至所述更新请求中，对所述更新请求进行提交后，动态载入的所述网页前端程序或软件代理人程序即可根据所述更新请求中的所述版本信息或所述装置规格信息，从第一装置 5 的存储媒体中获取与所述版本信息或所述装置规格信息对应的一装置代码，并发送至第二装置 6。

于一较佳实施例中，风险扫描系统 1 是在第一装置 5 上运行，所述更新请求是由第二装置 6 发出至第一装置 5，于生成该更新请求时，一版本信息或一装置规格信息被提供至所述更新请求中。方案一，由运行于第二装置 6

上的软件系统产生所述更新请求，并将所需装置代码的一版本信息或第二装置 6 的装置规格信息填入更新请求中，通过呼叫风险扫描系统 1 所提供的用于提交一更新请求的应用程序界面，将所述更新请求发送至第一装置 5 上所运行的风险扫描系统 1 的代码发送模块 2 中。代码发送模块 2 获取所述更新请求后，即可从第一装置 5 的存储媒体中获取与所述版本信息或所述装置规格信息对应的装置代码，进而发送至第二装置 6，更新为第二装置 6 上所运行的装置代码。方案二，所述更新请求亦可由运行于第一装置 5 上的风险扫描系统 1 所生成，于生成该更新请求时，一版本信息或一装置规格信息被提供至所述更新请求中，代码发送模块 2 根据所述更新请求中的所述版本信息或所述装置规格信息，在第一装置 5 的存储媒体中获取与所述版本信息或所述装置规格信息对应的装置代码后，即可发送至第二装置 6，更新为第二装置 6 上所运行的装置代码。

于一较佳实施例中，风险扫描系统 1 是在有别于第一装置 5 和第二装置 6 的另一运算装置 11 上运行，所述更新请求是在第一装置 5 上生成的更新请求，于生成该更新请求时，一版本信息或一装置规格信息被提供至所述更新请求中，或者所述更新请求是由第二装置 6 产生并发出至第一装置 5 的更新请求，于生成该更新请求时，一版本信息或一装置规格信息被提供至所述更新请求中。方案一，所述更新请求由本身运行于第一装置 5 上的软件系统或者是用户透过动态载入的代码发送模块 2 的网页前端程序或软件代理人程序所生成，经由对风险扫描系统 1 提供的用于发送装置代码的一应用程序界面的呼叫，将所述版本信息或所述装置规格信息对应的装置代码，发送至所述另一运算装置 11，进而由代码发送模块 2 发送至第二装置 6，更新为第二装置 6 上所运行的装置代码。方案二，所述更新请求由本身运行于第一装置 5 上的软件系统或者是用户透过动态载入的代码发送模块 2 的网页前端程序或软件代理人程序所生成，经由对风险扫描系统 1 提供的用于提交更新请求的

一应用程序界面的呼叫，所述更新请求提交至风险扫描系统 1 的代码发送模块 2 中，代码发送模块 2 透过一授权的身分，以 SSH (Secure Socket Shell) 通讯协定的连线接入第一装置 5，根据所述更新请求中的所述版本信息或所述装置规格信息，以通过存取存储媒体的系统指令遍历存储媒体来找出装置代码后，透过 SCP (Secure Copy Protocol) 通讯协定的连线从第一装置 5 的存储媒体中获取所需的装置代码后，进而由代码发送模块 2 发送至第二装置 6，更新为第二装置 6 上所运行的装置代码。方案三，由运行于第二装置 6 上的软件系统产生所述更新请求，并将所需装置代码的一版本信息或第二装置 6 的装置规格信息填入更新请求中，通过呼叫风险扫描系统 1 所提供的用于提交一更新请求的应用程序界面，将所述更新请求发送至第一装置 5 上所运行的风险扫描系统 1 的代码发送模块 2 中。代码发送模块 2 获取所述更新请求后，从第一装置 5 的存储媒体中获取与所述版本信息或所述装置规格信息对应的装置代码，进而发送至第二装置 6，更新为第二装置 6 上所运行的装置代码。

于一较佳实施例中，所述版本信息和所述装置规格信息都是所述装置代码的元数据的一部分。所述装置规格信息包括所述装置代码所支持运行的装置的产品规格、硬体规格以及软韧体规格中至少一个。

上述更新请求由第一装置 5 所生成的技术手段所衍生的效益在于，第二装置 6 无需知道第一装置 5 及/或所述另一运算装置 11 的网路位置信息。第一装置 5 和所述另一运算装置 11 以推送的方式为第二装置 6 完成装置代码的更新，于一较佳实施例中，第二装置 6 的网路位置信息是由用户透过所述动态载入的网页前端程序或软件代理人程序的人机界面填入所述更新请求中，或第二装置 6 的网路位置信息是由风险扫描程序 1 收到更新请求后，由风险扫描程序 1 将第二装置 6 的网络位置信息写入更新请求；接着由代码发送模

组 2 依据更新请求里的网络位置信息，将装置代码传送给第二装置 6 做更新。这种以异步的方式完成装置代码的更新的方式，更新请求的发出和装置代码的接收是经由两条连接对象不同的连线来完成的，有别于传统意义上的 OTA 更新是由第二装置 6 本身建立连线至提供更新代码的服务器下载。

事实上，上述情景使得装置代码的更新不需要第二装置 6 本身下载。第一装置 5 或所述另一运算装置 11 在权限允许的情况下，均可以透过上述改进方法，发出更新请求至风险扫描系统 1，随后，风险扫描系统 1 依据第二装置 6 的网络位置信息，对该网络位置信息所指的装置 6 建立连线，然后将装置代码主动地传输给它完成更新。

所述网络位置信息可以单纯是一个 IP Address，所述风险扫描系统 1 和第二装置 6 之间有一个默认用于传送装置代码的通讯协定（装置所默认支持的 Port），在这样的情况下，风险扫描系统 1 只需要知道装置的 IP Address，就可以主动对其连线，然后传送更新的装置代码。另外，网络位置信息也可以是 IP Address 加上 Port，也即该网络位置信息里包含了网路通讯协定的指定信息，这样风险扫描系统 1 和第二装置 6 之间不需要有任何一个默认的网络的通讯协定，风险扫描系统 1 也可以根据 IP Address（位置）加上 Port（通讯协定）来建立第一装置 5 和第一装置 5 或所述另一运算装置 11 之间的连线，并传送更新的装置代码。其中，以异步的方式完成装置代码的更新之方法，并不以此为限，熟知本技艺人士可依据实际应用需求而进行任何均等的变更设计。

上述风险扫描系统 1 对第二装置 6 的网络位置信息的取得，有多种方式可以进行。方案一，第二装置 6 的用户将第二装置 6 的元数据注册登入于风险扫描系统 1 的资料库中，其中第二装置 6 的元数据包括第二装置 6 的网络

位置信息，风险扫描系统 1 即可从资料库中，透过对第二装置 6 的元数据的查找，找出第二装置 6 的网路位置信息；第二装置 6 的元数据也可以包括第二装置 6 的产品规格、硬体规格以及软韧体规格中至少一个，风险扫描系统 1 可以透过更新请求中所包括的信息（装置代码所支持的产品规格、硬体规格以及软韧体规格等）对资料库做查找。方案二，风险扫描系统 1 和第二装置 6 同处在可以群播（Multicast）封包进行交互的网路环境中，风险扫描系统 1 可以周期性地发出“对装置进行查找的群播封包”至网路中，当第二装置 6 是具备支持该群播封包的通讯协定之装置时，收到该群播封包后，第二装置 6 即可将本身的网路位置信息，以及其产品规格、硬体规格及软韧体规格中至少一个，写入一回应用的群播封包并发出至网路环境，风险扫描系统 1 收到后，即可对第二装置 6 的网路位置信息及其产品规格、硬体规格及软韧体规格有所掌握，并登录至资料库中。

于一较佳实施例中，风险扫描系统 1 运行于第一装置 5 或另一运算装置 11，风险扫描系统 1 的代码发送模块 2 获取一更新请求时，即可依所述更新请求中所包括的版本信息和装置规格信息（产品规格、硬体规格及软韧体规格的至少一个），获取所需的装置代码外，亦可透过装置规格信息对上述所述的资料库进行查找，定位出第二装置 6 的网路位置信息后，将装置代码发出给第二装置 6，更新第二装置 6 上所运行的装置代码。

于一较佳实施例中，代码发送模块 2、更新记录生成模块 3、扫描结果通知模块 4 作为集成至风险扫描系统 1 中的处理单元，每个处理单元可以提供至少一个函式来实现与其它处理单元之间的交互，当一处理单元需要对另一处理单元发出请求时，得以将请求的内容作为参数，以函数调用的方式，将请求的内容输入至另一处理单元，该另一处理单元收到所述请求的内容后，即可依据所述请求的内容，为所述请求提供服务。于另一较佳实施例中，每

个处理单元也可以藉由网络联机或行程间通讯（Inter-process communication）等方式来实现与其它处理单元之间的交互，当一处理单元需要对另一处理单元发出请求时，该处理单元可以对该另一处理单元建立一TCP/UDP Socket 连线，通过彼此约定好的通讯协议，将请求的内容传送至该另一处理单元，或者是通过以部分内存共享所实作的行程间通讯机制，将请求的内容发送至该另一处理单元，使得该另一处理单元得以收到所述请求的内容，依据所述请求的内容，为所述请求提供服务；其中，如何将一请求提供至一处理单元，以及处理单元如何接收该请求的实施方式，并不以此为限，熟知本技艺人士可依据实际应用需求而进行任何均等的变更设计。

于另一较佳实施例中，所述更新请求是由风险扫描系统 1 直接生成后，提交予代码发送模块 2。其中，风险扫描系统 1 可以根据一设定档的内容来生成所述更新请求并提交予代码发送模块 2，所述设定档的内容可由包括上述从第一装置 5 获取一装置代码，并将所述装置代码发送至第二装置 6 的所需相关信息所组成。其中，所述相关信息包括第一装置 5 及/或第二装置 6 的网路位置信息、第一装置 5 及/或第二装置 6 的授权身分、版本信息及/或装置规格信息等，但不限于此。其中所述设定档可以在部署风险扫描系统 1 时，由风险扫描系统 1 的管理者设置予风险扫描系统 1，或者是在风险扫描系统 1 已在线运营时，由风险扫描系统 1 的管理者及/或其用户，通过风险扫描系统 1 的人机操作介面上的操作设置，提供至风险扫描系统 1 中。

综合以上所述，更新请求内容的生成、传输，以及代码发送模块 2 对更新请求的获取方法，并不以此为限，熟知本技艺人士可依据实际应用需求而进行任何均等的变更设计。

于一较佳实施例中，代码发送模块 2 获取所述更新请求，除了将装置代

码从第一装置 5 传送至第二装置 6，可进一步将所述装置代码储存于资料库或一档案服务器中，并请求更新记录生成模块 3 在风险扫描系统 1 的资料库中，建立一更新记录。方案一，风险扫描系统 1 运行于第一装置 5 中，所述更新记录中除了包括装置代码的版本信息、装置代码所支持的装置规格信息，装置代码于所述档案服务器中的储存位置信息外，亦包括一关系记录，所述关系记录包括第二装置 6 的元数据。方案二，风险扫描系统 1 运行于第二装置 6 中，所述更新记录中除了包括装置代码的版本信息、装置代码所支持的装置规格信息、装置代码于所述档案服务器中的储存位置信息外，亦包括一关系记录，所述关系记录包括第一装置 5 的元数据。方案三，风险扫描系统 1 运行于有别于第一装置 5 和第二装置 6 的另一运算装置 11 中，所述更新记录中除了包括装置代码的版本信息、装置代码所支持的装置规格信息、装置代码于所述档案服务器中的储存位置信息外，亦包括一关系记录，所述关系记录包括第一装置 5 的元数据及第二装置 6 的元数据。其中第一装置 5 的元数据包括第一装置 5 的网路位置信息以及第一装置 5 的用户、运营者及/或管理者的帐号信息，第一装置 5 的元数据可以包括第一装置 5 的网路位置信息以及第一装置 5 的用户、运营者及/或管理者的帐号信息。

于一较佳实施例中，第一装置 5 及/或第二装置 6 是一嵌入式系统装置、服务器装置、物联网感测设备、网络通讯设备，或任一具联网能力的计算机装置。

进一步的，所述装置代码是从第一装置 5 所获取，所述装置代码包含的至少一软件代码中，包含至少一二进制代码。

所述一种装置代码风险扫描方法，实现了风险扫描系统 1 实现了从第一装置 5 获取装置代码，并进而能对第二装置 6 进行装置代码更新，使装置代

码成为第二装置 6 在线运行时所执行的代码；在第一装置 5 和第二装置 6 是离线的环境下，实施装置代码风险扫描方法的风险扫描系统 1，能为第一装置 5 和第二装置 6 进行所述装置代码的风险扫描，亦即，藉由对储存于所述档案服务器里的装置代码进行代码成份分析。在上述方法下，第一装置 5 和第二装置 6 是在线的环境下，风险扫描系统 1 也能对为第一装置 5 和第二装置 6 进行装置代码的风险扫描，也即在线和离线的环境下均包含于装置代码风险扫描方法之中。

于一较佳实施例中，从第一装置 5 所获取的装置代码是以软件代码包裹的型态获取，亦即将装置代码包装至一软件代码包裹中；所述软件代码包裹的型态，可以包括一压缩文件，该压缩文件中包含所述装置代码所包含的所有软件代码。于另一较佳实施例中，所述装置代码是以系统映像文件的型态获取，所述系统映像文件中包含所述装置代码所包含的所有软件代码。

于一较佳实施例中，不论是以系统映像文件或软件代码包裹的型态，风险扫描系统 1 的代码发送模块 2 获取装置代码，即可对所述装置代码所包含的所有软件代码进行扫描。要扫描时，将装有所述装置代码的系统映像文件挂载至内存或是由硬盘内存分割出的扇区（如果是 zImage，可将以解压缩的方式，解压缩其内容至一文件夹中），或者是将装有所述装置代码的软件代码包裹解压缩至硬盘内存的一指定文件夹中，接着即可以将所述装置代码的完整内容储存至一档案服务器。对储存于所述档案服务器上的装置代码进行档案和目录的遍历，即均等于对所述系统映像文件和所述软件代码包裹所含的成份组成进行扫描。依据遍历的结果，掌握到所述装置代码的档案和目录结构后，即可与已知操作系统核心、驱动程序、应用程序、常用软件组件及/或类别库的档案和目录结构进行比对，比对出档案和目录结构相符合的操作系统核心、驱动程序、应用程序、常用软件组件及/或类别库。依上述程

序，风险扫描系统 1 即可在收集到所述装置代码后，扫描和剖析出所述装置代码中所含的软件代码的一组成清单。该组成清单可由包括以操作系统核心、驱动程序、应用程序、常用软件组件及/或类别库等型态存在的各个软件代码之元数据（所述元数据为描述软件代码相关信息的数据，例如各软件代码的名称等描述信息，皆可为一种元数据的态样）所组成，其中该组成清单的内容里亦可包含所述装置代码本身的元数据（所述元数据为描述装置代码相关信息的数据）。

于一较佳实施例中，依据所述装置代码所包括的所述至少一软件代码的组成清单，风险扫描系统 1 即可对所述组成清单中所含各个软件代码所相对应的 CVE 列表进行监控（例如针对 Linux Kernel，即对 Linux Kernel 所对应的 CVE 列表监控），藉由监控所述 CVE 列表的异动来侦测代码分析事件。当有一个漏洞被新增至列表、相对于该漏洞的补丁代码被提供并新增至该漏洞纪录，或者是该漏洞的补丁代码有所更新，导致该列表的内容出现异动时，即可触发出一代码分析事件；其中，补丁代码是风险代码所包括的一种态样，但并不以此为限，针对风险代码其中一种态样的恶意软件代码，熟知本技艺人士可依据实际应用需求而进行任何均等的变更设计。相对应于所述风险代码的所述代码分析事件是在所述风险代码被新增或被更新时所触发，所触发的事件得以由风险扫描系统 1 所接收。其中，CVE 列表是本文所述风险代码登录列表的一种实施态样，并不以此为限，熟知本技艺人士可依据实际应用需求而对不同形式的风险代码登录列表提供任何均等的变更设计。

于一较佳实施例中，当一补丁代码被新增或更新，因而导致相对应于所述补丁代码的一代码分析事件被触发，风险扫描系统 1 将得以从储存着所述补丁代码的存储媒体中，将所述补丁代码取出；其中，所述存储媒体可以和储存所述装置代码的所述档案服务器为同一存储媒体，或者是另一存储媒体。

于另一较佳实施例中，当风险扫描系统 1 监控到一补丁代码被新增或更新时，即可先将储存于另一存储媒体(例如:发布补丁代码的 GIT hub)中的所述补丁代码的源代码先行取出并予以编译，并将编译后的结果(二进制代码或中间码)储存于所述档案服务器，在此情况下，先行编译后的结果，可视为补丁代码整体的一部分，则风险扫描系统 1 在成份比对中，是从所述档案服务器及所述另一存储媒体中，将整体的补丁代码(包含源代码、二进制代码及/或中间码)取出。上述对风险代码登录列表之监控和取码之方法，并不以此为限，熟知本技艺人士可依据实际应用需求而进行任何均等的变更设计。

于一较佳实施例中，在风险扫描系统 1 取出所述补丁代码后，即可对所述补丁代码和所述装置代码中相对应的至少一软件代码进行成份内容的比对。当所述比对的结果显示出所述至少一软件代码包含至少一安全风险时，即可请求扫描结果通知模块 4，就所述安全风险发出扫描结果。

于一较佳实施例中，所述扫描结果包括一扫描状态通知信息及/或一扫描报告，所述发出一扫描结果，是指透过至少一网路通信渠道，例如包括电子邮件、手机推播通知、手机简讯通知、网页推播等网络通信渠道，向第一装置 5 和第二装置 6 的用户、运营者或管理者中的至少一人，发出所述扫描状态通知信息及/或所述扫描报告；其中，所述扫描报告用于展示至少一软件代码与至少一风险代码的成份内容比对结果。补丁代码是风险代码所包含的其中一种型态，补丁代码本身之所以存在，其所表示的就是所述装置代码所含的软件代码中，有着一相对应的已知或新发现的漏洞，而所述补丁代码即为针对该漏洞做修正的代码，若是所述补丁代码和所述软件代码的成份内容比对结果，显示出所述软件代码的成份内容并未包含所述的补丁代码，即表示所述装置代码中仍存在所述的漏洞，不肖人士即可利用所述漏洞对执行所述装置代码，且正在线运行所述装置代码的第一装置 5 及/或第二装置 6 进

行攻击，亦即所述漏洞的存在是包括第一装置 5 或第二装置 6 的风险。据此，扫描报告的内容所展示的成份内容比对结果可包括“所述至少一风险代码的描述信息”、“所述至少一软件代码的描述信息”、“所述装置代码的描述信息”、“所述漏洞的描述信息”、“所述风险的描述信息”、“所述装置代码及/或所述至少一软件代码所含的漏洞数量”、“所述装置代码及/或所述至少一软件代码的安全等级”，及/或是“所述至少一软件代码是否包含所述至少一风险代码的判断结果”等，但不以此为限。扫描状态通知信息即为就所述扫描结果的完成状态，而对相关人士所发出的通知信息，亦即透过至少一网路通信渠道，就所述扫描结果的完成状态，对所述第一装置 5 和所述第二装置 6 的用户、运营者或管理者中的至少一个提供扫描状态的通知，其中，扫描状态通知信息的内容可包括“所述扫描报告及/或其内容的描述信息”及/或“所述扫描报告的完整或部份内容”等，但不以此限。

于一较佳实施例中，当风险代码的型态是一恶意软件代码，所述恶意软件代码所表示的则是一已知漏洞的代码。亦即，若是所述恶意软件代码和所述软件代码的成份内容比对结果，显示出所述软件代码的成份内容仍然包含所述的恶意软件代码，即表示所述装置代码中仍存在所述的漏洞，而需发出扫描结果。

于一较佳实施例中，扫描结果通知模块 4 可以从风险扫描系统 1 的资料库中，调取出所述装置代码的更新记录，并且从更新记录的内容里，查找出一关系记录，依据所述关系记录所记载的第一装置 5 及/或第二装置 6 的用户、运营者或管理者中的至少一个的用户帐号信息，透过该至少一用户帐号信息，对第一装置 5 及/或第二装置 6 的用户、运营者及/或管理者中的至少一位发出扫描结果。亦即，根据所述至少一用户帐号信息，确认出所述用户、运营者及/或管理者中的至少一位的电子邮件地址及/或手机号码，透过电子

邮件、手机推播通知、手机简讯通知等网络通信渠道，向所述用户、运营者及/或管理者发出扫描结果（扫描报告及/或扫描状态通知信息）。

于一较佳实施例中，扫描结果通知模块 4 可以在所述用户、运营者及/或管理者于第一装置 5 或第二装置 6 的风险扫描系统 1 的网页前端程序时，透过所述网页前端程序，将扫描结果后端发出至所述网页前端程序。

上述扫描结果、扫描报告和扫描状态通知信息的内容，以及扫描结果的发送方式，不以此为限，熟知本技艺人士可依据实际应用需求而进行任何均等的变更设计。

于一较佳实施例中，风险扫描系统 1 在获取装置代码前，即可对至少一风险代码登录列表（例如：不同软件专案的 CVE 列表）的内容进行读取，依据所述至少一风险代码登录列表的内容中所载的漏洞纪录，找出所述补丁代码的发布来源（例如：用于发布补丁代码的 GIT hub），从储存于另一存储媒体（例如：用于发布补丁代码的 GIT hub）将所述补丁代码的源代码取出并予以编译，并将编译后的结果（二进制代码或中间码）储存于所述档案服务器，借此技术实施方式，将相对应于所述至少一风险代码登录列表的至少一补丁代码（风险代码的一种实施态样），预先搜集于档案服务器中。如此一来，在所述装置代码所包含的所述至少一软件代码的所述组成清单，经由对所述装置代码的剖析而取得时，风险扫描系统 1 即可依据所述组成清单中的各个软件代码，定位出与所述软件代码相对应的风险代码登录列表，进而从档案服务器中取出依据所述相对应的风险代码登录列表所预先搜集的风险代码来和所述装置代码中的各个软件代码进行成份内容的比对，即可取得针对整体装置代码的扫描结果。由上述可知，代码分析事件可以在不同情境下触发，其中至少包括：1）取得装置代码所含至少一软件代码的一组成清单时触发；

2) 至少一风险代码在相对应的风险代码登录列表中被新增时触发；或 3) 至少一风险代码在相对应的风险代码登录列表中被更新时触发，但是不以此为限，熟知本技艺人士可依据实际应用需求而进行任何均等的变更设计。另亦可知，所述至少一风险代码可以预先依据至少一风险代码登录列表而搜集至档案服务器外，亦可在一风险代码被新增或更新至所述至少一风险代码登录列表时所搜集，然而搜集风险代码的方式亦不以此为限，熟知本技艺人士可依据实际应用需求而进行任何均等的变更设计。

针对本文所述的「软件代码的成份内容」及「风险代码的成份内容」，其中所述「成份内容」所指的是包括“所述代码的代码组成内容里所含的程序指令”、“所述代码于内存中的储存结构”、“所述执行代码所需的环境设置及组态资料”；其中，所述代码的代码组成内容包括任一种供加载和执行用的二进制代码(Binary Code)、中间码，及/或任一种由计算机程序语言编写的计算机程序代码。另，本文所述的「安全风险」包括所述代码中含有漏洞、病毒及/或恶意软件的风险，及/或是任一种让所述代码执行不可预期逻辑运算的风险。上述以风险代码和软件代码的比对来扫描一安全风险的方法，并不以此为限，熟知本技艺人士可依据实际应用需求而进行任何均等的变更设计。

如图 1 所示，S3 的所述当检测到所述装置代码中存在安全风险，于检测安全风险前的代码成份分析，具体包括以下步骤：

- S31、撷取相对应于所述风险代码的至少一第一成份特征；
- S32、撷取自相对应于所述至少一软件代码的至少一第二成份特征；
- S33、对至少一第一成份特征和至少一第二成份特征进行比对。

进一步的，S31 中所述第一成份特征是藉由对相对应于所述风险代码的

代码组成内容及/或代码执行结果进行剖析后所得；其中，所述代码组成内容包括所述风险代码及/或所述风险代码编译后的第一中间代码，所述代码执行结果则包括对所述风险代码及/或所述第一中间代码做模拟执行时，所述风险代码及/或所述第一中间代码在模拟执行过程中所显露出的语义信息。

进一步的，S32 中所述至少一第二成份特征是藉由对相对应于所述至少一软件代码的至少一代码组成内容及/或至少一代码执行结果进行剖析后所得；其中，所述至少一代码组成内容包括至少一二进制代码及/或所述至少一二进制代码反组译后的至少一第二中间代码，所述至少一代码执行结果则包括对所述至少一二进制代码及/或所述至少一第二中间代码做模拟执行时，所述至少一二进制代码及/或所述至少一第二中间代码在模拟执行过程中所显露出的语义信息。

进一步的，所述其中所述第一中间代码及/或所述至少一第二中间代码的程序语言结构是由一中间语言（intermediate language）、一中间表示（intermediate presentation）、一结构化语言（structured language），及/或一结构化协议（structured protocol）所宣告而成。

于一较佳实施例中，所述风险代码的种类是包括与所述至少一软件代码所关联的一补丁代码、恶意程序代码，及/或任一种用于修正或产生一软件漏洞或软件病毒的代码。

于一较佳实施例中，所述风险代码的所述代码分析事件是在所述风险代码被新增或被更新至一风险代码登录列表（例如：CVE 列表）时所触发。

于一较佳实施例中，所述代码分析事件触发前，进一步包括：所述风险扫描系统 1 依据所述至少一软件代码的一组成清单，对至少一代码分析事件进行侦测。相对应于所述风险代码的所述代码分析事件是所述至少一代码分析事件的其中之一。

于一较佳实施例中，所述装置代码的成份组成可以由包括系统核心、驱动程序、应用程序、组件，及/或类别库等不同型态存在的软件代码所

组成。各软件代码的代码组成内容则可包括一些 Script、二进制代码及/或是中间码。所以至少一软件代码，可以视其为装置代码中的一部分作理解。而至少一代码组成内容，可以视其为所述至少一软件代码中的一部分作理解。

一个装置里所含的该至少一软件代码，一般来说是由一个清单所组成，例如：其中可能包含 Linux Kernel、OpenSSL、sqlite 等组件。这些组件随着不断地被检验，都有漏洞被发现以及相对应的补丁代码被发布，然后新增或更新至网路上的 CVE 列表（CVE repository）和 GIT Hub。

这些漏洞和补丁代码由所属单位或组织新增或更新至网路上的 CVE 列表和 GIT Hub 时，并不会通知本文所述的风险扫描系统 1。因此代码分析事件要能够被触发，即表示在触发前，风险扫描系统 1 应依据装置代码的组成清单，向 Linux Kernel、OpenSSL、sqlite 等 CVE 列表和 GIT Hub 进行监控，以侦测这些代码分析事件。

这样带来的技术效果是，该风险扫描系统 1 可以在一漏洞和补丁代码被新增或更新至网络上的风险代码登录列表（例如：CVE 列表）时，即时地完成装置代码的代码安全检测工作。

进一步的，所述组成清单是在所述装置代码被提供至所述风险扫描系统 1 时，由所述风险扫描系统 1 对所述装置代码的成份组成进行扫描及/或剖析后所得。

所述装置代码可以是单独的一个 .o 档（目的档）、.img 档（系统映像档）、.so 档（程序库），或者是一个 .zip or .gz 压缩档（内容包含整个装置所需的 .o 和 .so 档，并且压缩档中也保有该些档案的路径结构）。

以一个装置的整体装置代码来说，其中所包含的软件代码的档案是很多的，各软件代码以不同组件（例如：Linux Kernel、OpenSSL、sqlite等）的型态，组合在装置代码中。各软件代码的档案会存在不同的路径位置。有不同方式可以取得装置代码所包含的软件代码的组成清单，一种是针对档案路径的信息去扫描整个装置代码，作为不同组件的软件代码，其相关档案会放在不同的位置，如此可基本确定出装置代码中含有哪些组件。另外，也可以去读取各软件代码的档案的内容，比对看看该些档案内容中是否存在特定组建的一些特征来掌握组件清单，例如在读取一软件代码所含的代码档案中的代码组成内容时，可以和Linux Kernel、OpenSSL、sqlite等该些已知软件的已知代码片段做比对，依据比对结果，即可确定出装置代码中含有那些组件。扫描及/或剖析装置代码的成份组成以取得装置代码中各软件代码的组成清单之方法，并不以此为限，熟知本技艺人士可依据实际应用需求而进行任何均等的变更设计。

于一较佳实施例中，补丁代码的代码组成内容包含一 Javascript 所编写，内含 Javascript 代码的档案。该补丁代码的作用在于修正装置代码所包含的一软件代码的一漏洞。风险扫描系统 1 首先可藉由所述 Javascript 档案的档名，定位出该档名所对应的 Javascript 档案是在该软件代码的代码组成内容中的哪个位置。分别对该补丁代码的 Javascript 档案和该软件代码的相对应 Javascript 档案的内容进行读取后，就该两个档案所含的成份内容进行比对，亦即，比对两个档案的内容中，是否包含修正后的代码片段，以修正后的代码片段作为比对的成份特征，比对结果相符表示该软件代码不含该漏洞，不相符表示该软件代码含有该漏洞。

于一较佳实施例中，比对用的成份特征，除了是以代码中所含的片段作为特征外，亦可以补丁代码和软件代码在内存中的储存结构及/或补丁

代码和软件代码的环境设置及组态信息来作为比对用的成份特征。例如：一补丁代码的代码组成内容中，新增了一个档案，而这个档案的档名，并不存在于相对应软件代码的代码组成内容中，及/或补丁代码在环境设置和组态上加入了一新的参数，而此参数不存在于相对应软件代码的环境设置和组态里，即可谓所述软件代码的成份内容里，并不包含该补丁代码，因而所述软件代码中仍存在着该补丁代码所对应的漏洞。

依上例，用于比对的补丁代码的代码片段、文件名结构及/或组态内容是成份内容比对里的第一成份特征。用于比对的软件代码的代码片段、文件名结构及/或组态内容是成份内容比对里的第二成份特征。通过剖析代码组成内容而得出的成份特征进行比对的方法，并不以此为限，熟知本技艺人士可依据实际应用需求而进行任何均等的变更设计。

于一较佳实施例中，一软件代码的代码组成内容包含一内含二进制代码的第一档案，而所述第一档案的档名及其于储存结构中的相对位置可对应到一补丁代码所含的内含以 C/C++ 源代码编写的第二档案。所述第二档案包含用于修正一漏洞的代码。在此情况下，先将所述第一档案反汇编成第一中间代码（以 LLVM 的 IR 为中间代码表示形式的代码），亦将第二档案进行编译后，再反汇编成第二中间代码（以 LLVM 的 IR 为中间代码表示形式的代码）。进而即可针对所述第一中间代码和所述第二中间代码进行模拟执行，亦即通过读取所述第一中间代码和所述第二中间代码中的程序指令，喂入仿真的参数（parameter）后，依据所述读取的程序指令进行逻辑运算。当所有程序指令都被执行过后，即可依据程序指令的执行过程中各指令的执行历程、函数呼叫的输出、输入及/或执行顺序来得到模拟执行过程中所显露出的语义信息；其中，本文所述的「语义信息」包括程序运行时的内存及/或中间变量的取值，及/或模拟执行过程中调用的指令、

函数及其输出、输入值。对第一中间代码语义信息和第二中间代码语义信息的进行比对而得出一相似度，即可依所述相似度决定出第一中间代码和第二中间代码的代码片段是否相符，进而判断所述第一档案是否含有第二档案中用于修正所述漏洞的代码。其中，第一中间代码语义信息和第二中间代码语义信息全部内容所构成的成份特征，完全包含于彼此的语义信息中，即可谓相似度为 100%，仅一部分内容所构成的成份特征的包含于彼此的语义信息中，即可为所述部分所占全部内容的比例，即为其相似度，据此可得到 0%至 100%的相似度结果，相似度超过所设定的一阈值即可表示第一档案包含第二档案的代码。所述阈值是用于判断第二档案的代码是否包含于第一档案的参考数值，例如：所述阈值设定为 90%，即表示当相似度高于 90%，则第一档案包含第二档案的代码，反之则不包含。

于一较佳实施例中，一软件代码的代码组成内容包含一内含中间码（Java bytecode）的第一档案，而所述第一档案的档名及其于储存结构中的相对位置可对应到一补丁代码所含的内含以 Java 源代码编写的第二档案。所述第二档案包含用于修正一漏洞的代码。在此情况下，将所述第二档案编译为中间码（Java bytecode）后，透过模拟执行的来取得其语义信息，进而得以透过语义信息里所含从内存及/或中间变量取出的值，及/或模拟执行过程中调用的指令、函数及其输出、输入值的成份特征来比对出所述第一档案是否含有所述第二档案中用于修正所述漏洞的代码。

以上所述以模拟执行得到的语义信息的成份特征进行比对的方法，并不以此限，熟知本技艺人士可依据实际需求而进行任何均等的变更设计。

如图 5 所示，本实施例还提供一种装置代码风险扫描运算装置 11，包

括代码发送模块 21、更新记录生成模块 31 以及扫描结果通知模块 41；

所述代码发送模块 21 用于获取一装置代码，所述装置代码是由第一装置 5 所获取，并将所述装置代码自第一装置 5 发送至第二装置 6；其中，所述装置代码包括至少一个软件代码；

所述更新记录生成模块 31 用于生成一更新记录；其中，所述更新记录中包括所述装置代码与所述第一装置 5 及/或所述第二装置 6 之间的关系记录；

所述扫描结果通知模块 41 用于当检测到所述装置代码中存在安全风险时，根据所述更新记录向所述第一装置 5 及/或所述第二装置 6 发出扫描结果。

在扫描结果显示所述至少一软件代码包含至少一安全风险时，所述扫描结果通知模块 41 还用于发出扫描结果，扫描结果通知模块 41 透过至少一网路通信渠道，向所述第一装置 5 和第二装置 6 的用户、运营者或管理者的至少一人，发出所述扫描结果。

于一较佳实施例中，所述运算装置 11 是一嵌入式装置。所述代码发送模块 21、更新记录生成模块 31 及/或扫描结果通知模块 41，是以硬件描述语言所设计而可被运算装置 11 的集成电路单元或者是以软件代码的形式集成至运算装置 11 的嵌入式系统中。通过运行于运算装置 11 里的嵌入式系统对代码发送模块 21、更新记录生成模块 31 及扫描结果通知模块 41 进行驱动。

于另一较佳实施例中，所述运算装置 11 是一服务器，所述代码发送模块 21、更新记录生成模块 31 及/或扫描结果通知模块 41 是以软件代码的形式集成至一软件系统，所述软件系统通过内建或安装的方式，提供至运算装置 11 中运行，通过运行于运算装置 11 里的软件系统对代码发送模

块 21、更新记录生成模块 31 及扫描结果通知模块 41 进行驱动。

于另一较佳实施例中，所述运算装置 11 是由分散的服务器所构成，所述代码发送模块 21、更新记录生成模块 31 及/或扫描结果通知模块 41 是以软件代码的形式集成至一分散式软件系统，所述分散式软件系统部署至所述分散的服务器中运行，组成一运算装置 11。通过运行于运算装置 11 里的分散式软件系统对代码发送模块 21、更新记录生成模块 31 及扫描结果通知模块 41 进行驱动。

上述以不同形式的硬件和软件结合组成运算装置 11 之方式，并不以此为限，熟知本技艺人士可依据实际应用需求而进行任何均等的变更设计。

进一步的，结合图 2，所述风险扫描系统 1 包括第一特征提取单元、第二特征提取单元和特征比对单元；

所述第一特征提取单元，用于撷取相对应于所述至少一风险代码的至少一第一成份特征；

所述第二特征提取单元，用于撷取自相对应于所述至少一软件代码的至少一第二成份特征；

所述特征比对单元，用于对至少一第一成份特征和至少一第二成份特征进行比对。

再进一步的，所述第一特征提取单元或第二特征提取单元包括至少一剖析单元和至少一撷取单元；

至少一剖析单元，用于对相对应于所述至少一风险代码的代码组成内容及/或代码执行结果进行剖析后得到所述至少一第一成份特征，及/或对相对应于所述至少一软件代码的代码组成内容及/或代码执行结果进行剖析后得到所述至少一第二成份特征；

至少一摄取单元，用于摄取剖析后所得到的所述至少一第一成份特征或所述至少一第二成份特征。

结合图 3，所述一种装置代码风险扫描运算装置 11 还包括至少一侦测单元；

所述至少一侦测单元，用于依据所述装置代码所包括的所述至少一软件代码的组成清单，对所述组成清单中所含各个软件代码所相对应的风险代码登录列表（例如：CVE 列表）进行监控，藉由监控所述风险代码登录列表的异动来侦测代码分析事件。

综上，本发明公开一种装置代码风险扫描方法、系统和运算装置 11，通过对一在线运行的装置的装置代码获取、对一在线运行的装置的装置代码更新、对风险代码和所述装置代码成份内容的比对，以及为所述该等装置发出扫描结果，无论所述该等装置是否离线，网路状态是否正常，运算能力是否不足，也能对所述该等装置进行风险扫描，据以实现对装置代码的风险防控。

上列详细说明是针对本发明可行实施例的具体说明，所述实施例并非用以限制本发明的保护范围，凡未脱离本发明所为的等效实施或变更，均应包含于本发明的保护范围中。

权利要求

1. 一种基于装置代码的风险扫描方法，其特征在于，包括：

获取一装置代码，所述装置代码是从第一装置所获取，并将所述装置代码自第一装置发送至第二装置；其中，所述装置代码包括至少一软件代码；

生成一更新记录；其中，所述更新记录中包括所述装置代码与所述第一装置及/或所述第二装置之间的关系记录；

当检测到所述装置代码中存在安全风险时，根据所述更新记录向所述第一装置及/或所述第二装置发出扫描结果。

2. 如权利要求 1 所述的基于装置代码的风险扫描方法，其特征在于：所述发出扫描结果，是指透过至少一网路通信渠道，向所述第一装置和第二装置的用户、运营者或管理者中至少一人，发出一扫描结果的通知。

3. 如权利要求 1 所述的基于装置代码的风险扫描方法，其特征在于，所述至少一软件代码包含至少一二进制代码。

4. 如权利要求 1 所述的基于装置代码的风险扫描方法，其特征在于，所述获取装置代码，具体包括：

依据一更新请求，从所述第一装置的一存储媒体中获取所述装置代码。

5. 如权利要求 4 所述的基于装置代码的风险扫描方法，其特征在于，所述获取装置代码的方法还包括：

当获取所述更新请求时，根据所述更新请求中的一版本信息或一装置规格信息，在所述存储媒体中获取与所述版本信息或所述装置规格信息对应的装置代码，作为所述装置代码；其中，所述装置规格信息包括一装置的产品规格、硬体规格以及软韧体规格中至少一个。

6. 如权利要求 4 所述的基于装置代码的风险扫描方法，其特征在于，所述将所述装置代码发送至第二装置，具体包括：

根据所述更新请求所包括的第二装置的网络位置信息，将所述装置代码发送至所述第二装置。

7. 如权利要求 1 所述的基于装置代码的风险扫描方法，其特征在于，所

述检测到所述装置代码中存在安全风险，具体包括：

当至少一代码分析事件触发时，将至少一风险代码与所述至少一软件代码进行成份内容的比对；其中，所述至少一风险代码包括与所述至少一软件代码关联的补丁代码、恶意程序代码以及任意一种由计算机程序语言编写的计算机程序代码中的至少一个。

8. 如权利要求 7 所述的基于装置代码的风险扫描方法，其特征在于：所述至少一风险代码是依据至少一风险代码登录列表而被预先搜集，或者是在一风险代码被新增或更新至所述至少一风险代码登录列表时所搜集。

9. 如权利要求 7 所述的基于装置代码的风险扫描方法，其特征在于：所述至少一代码分析事件是在包括取得所述至少一软件代码的一组成清单时所触发，或者是所述至少一风险代码被新增或被更新时所触发。

10. 如权利要求 7 所述的基于装置代码的风险扫描方法，其特征在于，所述将所述至少一风险代码与所述至少一软件代码进行比对，具体包括：

 擷取相对应于所述至少一风险代码的至少一第一成份特征；

 擷取相对应于所述至少一软件代码的至少一第二成份特征；

 比对所述至少一第一成份特征和所述至少一第二成份特征。

11. 如权利要求 10 所述的基于装置代码的风险扫描方法，其特征在于：所述至少一第一成份特征是藉由对相对应于所述至少一风险代码的代码组成内容及/或代码执行结果进行剖析后所得。

12. 如权利要求 11 所述的基于装置代码的风险扫描方法，其特征在于，所述代码组成内容包括所述至少一风险代码及/或所述至少一风险代码编译后的至少一第一中间代码，所述代码执行结果则包括对所述至少一风险代码及/或所述至少一第一中间代码做模拟执行时，所述至少一风险代码及/或所述至少一第一中间代码在模拟执行过程中所显露出的语义信息。

13. 如权利要求 10 所述的基于装置代码的风险扫描方法，其特征在于：所述至少一第二成份特征是藉由对相对应于所述至少一软件代码的至少一

代码组成内容及/或至少一代码执行结果进行剖析后所得。

14. 如权利要求 13 所述的基于装置代码的风险扫描方法，其特征在于：所述至少一代码组成内容包括至少一二进制代码及/或所述至少一二进制代码反组译后的至少一第二中间代码，所述至少一代码执行结果则包括对所述至少一二进制代码及/或所述至少一第二中间代码做模拟执行时，所述至少一二进制代码及/或所述至少一第二中间代码在模拟执行过程中所显露出的语义信息。

15. 如权利要求 12 或 14 所述的基于装置代码的风险扫描方法，其特征在于：所述中间代码的程序语言结构是由一中间语言、一中间表示、一结构化语言，及/或一结构化协议所宣告而成。

16. 如权利要求 7 所述的基于装置代码的风险扫描方法，其特征在于：所述代码分析事件触发前，还包括：

依据所述至少一软件代码的组成清单，对至少一代码分析事件进行侦测，相对应于所述至少一风险代码的所述代码分析事件是所述至少一代码分析事件的其中之一。

17. 如权利要求 9 所述的基于装置代码的风险扫描方法，其特征在于：所述组成清单是在所述装置代码被获取时，对所述装置代码的成份组成进行扫描及/或剖析后所取得。

18. 如权利要求 17 所述的基于装置代码的风险扫描方法，其特征在于：所述组成清单包括所述装置代码本身的元数据及/或所述装置代码成份组成中所含的所述至少一软件代码的元数据。

19. 如权利要求 18 所述的基于装置代码的风险扫描方法，其特征在于：所述至少一软件代码是以包括系统核心、驱动程序、应用程序、组件，及/或类别库的型态存在于所述装置代码的成份组成中。

20. 如权利要求 17 所述的基于装置代码的风险扫描方法，其特征在于：依据所述组成清单，对所述组成清单中所含各个软件代码所相对应的风险

代码登录列表进行监控，藉由监控所述风险代码登录列表的异动来侦测代码分析事件。

21. 如权利要求 17 所述的基于装置代码的风险扫描方法，其特征在于，所述组成清单的获取方法具体包括：

所述装置代码是一系统映像档，对系统映像档中所含的成份组成进行扫描及/或剖析，辨识出存在于所述系统映像档中的所述至少一软件代码，进而得到所述至少一软件代码的所述组成清单；

或者所述装置代码是一软件代码包裹，对所述软件代码包裹中所含的成份组成进行扫描及/或剖析，辨识出存在于所述软件代码包裹中的所述至少一软件代码，进而得到所述至少一软件代码的所述组成清单。

22. 如权利要求 1 所述的基于装置代码的风险扫描方法，其特征在于，所述根据所述更新记录向所述第一装置及/或所述第二装置发出扫描结果，具体包括：

对所述更新记录进行查找，获取所述更新记录中的关系记录；

根据所述关系记录对所述第一装置和所述第二装置的用户、运营者或管理者的至少一个发出扫描结果。

23. 如权利要求 22 所述的基于装置代码的风险扫描方法，其特征在于，所述扫描结果包括扫描报告与扫描状态通知信息中至少一个；其中，所述扫描报告用于展示所述至少一软件代码与所述至少一风险代码的成份内容比对结果；所述扫描状态通知信息用于对所述第一装置和所述第二装置的用户、运营者或管理者中的至少一个提供扫描状态的通知。

24. 一种基于装置代码的风险扫描系统，其特征在于，包括：代码发送模块、更新记录生成模块以及扫描结果通知模块；

所述代码发送模块用于获取一装置代码，所述装置代码是从第一装置所获取，并将所述装置代码自第一装置发送至第二装置；其中，所述装置代码包括至少一个软件代码；

所述更新记录生成模块用于生成一更新记录；其中，所述更新记录中包括所述装置代码与所述第一装置及/或所述第二装置之间的关系记录；

所述扫描结果通知模块用于当检测到所述装置代码中存在安全风险时，根据所述更新记录向所述第一装置及/或所述第二装置发出扫描结果。

25. 如权利要求 24 所述的基于装置代码的风险扫描系统，其特征在于，还包括：第一特征提取单元、第二特征提取单元和特征比对单元；

所述第一特征提取单元，用于撷取相对应于至少一风险代码的至少一第一成份特征；

所述第二特征提取单元，用于撷取自相对应于所述至少一软件代码的至少一第二成份特征；

所述特征比对单元，用于对至少一第一成份特征和至少一第二成份特征进行比对。

26. 如权利要求 25 所述的基于装置代码的风险扫描系统，其特征在于，所述第一特征提取单元或第二特征提取单元包括至少一剖析单元和至少一撷取单元；

所述至少一剖析单元，用于对相对应于所述至少一风险代码的代码组成内容及/或代码执行结果进行剖析后得到所述至少一第一成份特征，及/或对相对应于所述至少一软件代码的代码组成内容及/或代码执行结果进行剖析后得到所述至少一第二成份特征；

所述至少一撷取单元，用于撷取剖析后所得到的所述至少一第一成份特征及/或所述至少一第二成份特征。

27. 如权利要求 24 所述的基于装置代码的风险扫描系统，其特征在于，还包括：至少一侦测单元，

所述至少一侦测单元，用于依据所述至少一个软件代码的组成清单，对组成清单中所含各个软件代码所相对应的风险代码登录列表进行监控，藉由监控所述风险代码登录列表的异动来侦测代码分析事件。

28. 一种基于装置代码的风险扫描的运算装置，其特征在于，包括：代码发送模块、更新记录生成模块以及扫描结果通知模块；

所述代码发送模块用于获取一装置代码，所述装置代码是从第一装置所获取，并将所述装置代码自第一装置发送至第二装置；其中，所述装置代码包括至少一个软件代码；

所述更新记录生成模块用于生成一更新记录；其中，所述更新记录中包括所述装置代码与所述第一装置及/或所述第二装置之间的关系记录；

所述扫描结果通知模块用于当检测到所述装置代码中存在安全风险时，根据所述更新记录向所述第一装置及/或所述第二装置发出扫描结果。