(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 108256334 B
(45)授权公告日 2019.06.04

(21)申请号 201810079188.1

(22)申请日 2018.01.26

(65)同一申请的已公布的文献号
申请公布号 CN 108256334 A

(43)申请公布日 2018.07.06

(73)专利权人 平安科技(深圳)有限公司
地址 518052 广东省深圳市福田区八卦岭八卦三路平安大厦六楼

(72)发明人 林嘉思

(74)专利代理机构 广州华进联合专利商标代理有限公司 44224
代理人 黄晶晶

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

(56)对比文件
CN 104699616 A,2015.06.10,
CN 103077348 A,2013.05.01,
US 9282114 B1,2016.03.08,
CN 107480531 A,2017.12.15,
CN 106487813 A,2017.03.08,

审查员 李婧雯

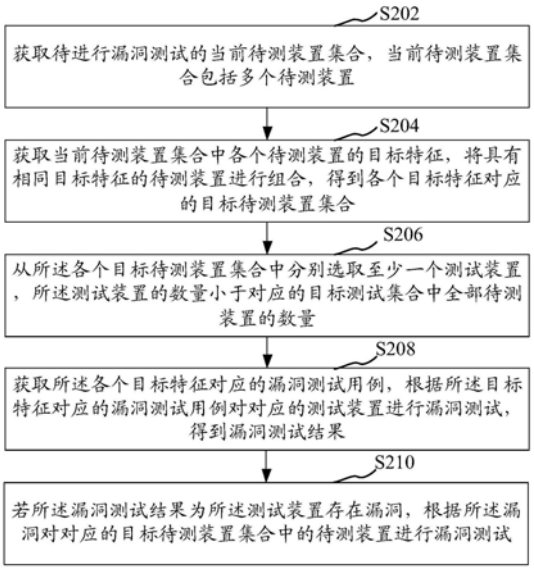
权利要求书2页 说明书12页 附图6页

(54)发明名称

漏洞测试方法、装置、计算机设备和存储介质

(57)摘要

本申请涉及一种漏洞测试方法、系统、计算机设备和存储介质。方法包括:获取待进行漏洞测试的当前待测装置集合,当前待测装置集合包括多个待测装置;获取当前待测装置集合中各个待测装置的目标特征,将具有相同目标特征的待测装置进行组合,得到各个目标特征对应的目标待测装置集合;从各个目标待测装置集合中分别选取测试装置,测试装置的数量小于对应的目标测试集合中全部待测装置的数量;获取各个目标特征对应的漏洞测试用例,根据目标特征对应的漏洞测试用例对对应的测试装置进行漏洞测试,得到漏洞测试结果;若漏洞测试结果为测试装置存在漏洞,根据漏洞对对应的目标待测装置集合中的待测装置进行漏洞测试。采用本方法能够提高漏洞测试效率。



CN 108256334 B

1.一种漏洞测试方法,所述方法包括:

获取待进行漏洞测试的当前待测装置集合,所述当前待测装置集合包括多个待测装置;

获取所述当前待测装置集合中各个待测装置的目标特征,将具有相同目标特征的待测装置进行组合,得到所述各个目标特征对应的目标待测装置集合;

从所述各个目标待测装置集合中分别选取至少一个测试装置,所述测试装置的数量小于对应的目标测试集合中全部待测装置的数量;

获取所述各个目标特征对应的漏洞测试用例,根据所述目标特征对应的漏洞测试用例对与所述目标特征对应的目标待测装置集合中选出的至少一个测试装置进行漏洞测试,得到相应的漏洞测试结果;

若所述漏洞测试结果为某一测试装置存在漏洞,根据所述漏洞对所述测试装置对应的目标待测装置集合中的待测装置进行漏洞测试。

2.根据权利要求1所述的方法,其特征在于,所述若所述漏洞测试结果为某一测试装置存在漏洞,根据所述漏洞对所述测试装置对应的目标待测装置集合中的待测装置进行漏洞测试的步骤包括:

若所述漏洞测试结果为某一测试装置存在漏洞,获取所述漏洞对应的测试特征;

根据所述测试特征得到对应的目标测试用例;

根据所述目标测试用例对对应的目标待测装置集合中的待测装置进行漏洞测试。

3.根据权利要求2所述的方法,其特征在于,所述漏洞对应的测试特征包括所述漏洞所在的当前代码对应的代码特征,所述根据所述测试特征得到对应的目标测试用例的步骤包括:

根据所述代码特征得到对应的目标测试用例。

4.根据权利要求3所述的方法,其特征在于,所述漏洞测试用例包括白盒测试用例,所述代码特征包括所述当前代码对应的控件标识,所述根据所述代码特征得到对应的目标测试用例的步骤包括:

根据所述控件标识以及所述白盒测试用例的测试参数构造黑盒测试用例,作为目标测试用例。

5.根据权利要求3所述的方法,其特征在于,所述漏洞测试用例包括白盒测试用例,所述代码特征包括所述当前代码对应的变量约束条件以及所述当前代码对应的控件标识,所述根据所述代码特征得到对应的目标测试用例的步骤包括:

根据所述控件标识以及所述变量约束条件构造黑盒测试用例,作为目标测试用例。

6.根据权利要求1～5任意一项所述的方法,其特征在于,所述方法还包括:

获取所述当前待测装置集合中各个待测装置的漏洞的危险度;

根据所述各个漏洞的危险度以及对应的待测装置的重要度得到所述当前待测装置集合的安全风险,所述安全风险与所述危险度呈正相关关系,所述安全风险与所述重要度呈正相关关系。

7.根据权利要求1～5任意一项所述的方法,其特征在于,所述目标特征包括域名特征,所述获取所述当前待测装置集合中各个待测装置的目标特征,将具有相同目标特征的待测装置进行组合,得到所述各个目标特征对应的目标待测装置集合的步骤包括:

获取所述当前待测装置集合中各个待测装置的域名，对所述各个待测装置的域名的无效信息进行过滤，得到域名特征；

将具有相同域名特征的待测装置进行组合，得到相同的域名特征对应的目标待测装置集合。

8.一种漏洞测试装置，所述装置包括：

当前集合获取模块，用于获取待进行漏洞测试的当前待测装置集合，所述当前待测装置集合包括多个待测装置；

组合模块，用于获取所述当前待测装置集合中各个待测装置的目标特征，将具有相同目标特征的待测装置进行组合，得到所述各个目标特征对应的目标待测装置集合；

选取模块，用于从所述各个目标待测装置集合中分别选取至少一个测试装置，所述测试装置的数量小于对应的目标测试集合中全部待测装置的数量；

测试装置测试模块，用于获取所述各个目标特征对应的漏洞测试用例，根据所述目标特征对应的漏洞测试用例对与所述目标特征对应的目标待测装置集合中选出的至少一个测试装置进行漏洞测试，得到相应的漏洞测试结果；

待测装置测试模块，用于若所述漏洞测试结果为某一测试装置存在漏洞，根据所述漏洞对所述测试装置对应的目标待测装置集合中的待测装置进行漏洞测试。

9.一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述计算机程序时实现权利要求1至7中任一项所述方法的步骤。

10.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现权利要求1至7中任一项所述的方法的步骤。

漏洞测试方法、装置、计算机设备和存储介质

技术领域

[0001] 本申请涉及安全技术领域，特别是涉及一种漏洞测试方法、装置、计算机设备和存储介质。

背景技术

[0002] 随着信息技术的发展，计算机设备提供的功能越来越多，由于系统设计或者编码的缺陷等导致的漏洞问题也越来越多。为了避免漏洞被有意或无意地利用，从而造成损失，需要对计算机系统进行漏洞测试。传统技术中，当需要对漏洞进行检测时，可以构造测试用例，然后将测试用例发送到对应的计算机设备上进行测试。然而，由于计算机功能多且代码复杂，测试用例数量大，导致漏洞测试时间长，测试效率低。

发明内容

[0003] 基于此，有必要针对上述技术问题，提供一种能够提高测试效率的漏洞测试方法、装置、计算机设备和存储介质。

[0004] 一种漏洞测试方法，所述方法包括：获取待进行漏洞测试的当前待测装置集合，所述当前待测装置集合包括多个待测装置；获取所述当前待测装置集合中各个待测装置的目标特征，将具有相同目标特征的待测装置进行组合，得到所述各个目标特征对应的目标待测装置集合；从所述各个目标待测装置集合中分别选取至少一个测试装置，所述测试装置的数量小于对应的目标测试集合中全部待测装置的数量；获取所述各个目标特征对应的漏洞测试用例，根据所述目标特征对应的漏洞测试用例对对应的测试装置进行漏洞测试，得到漏洞测试结果；若所述漏洞测试结果为所述测试装置存在漏洞，根据所述漏洞对对应的目标待测装置集合中的待测装置进行漏洞测试。

[0005] 在其中一个实施例中，所述若所述漏洞测试结果为所述测试装置存在漏洞，根据所述漏洞对对应的目标待测装置集合中的待测装置进行漏洞测试的步骤包括：若所述漏洞测试结果为所述测试装置存在漏洞，获取所述漏洞对应的测试特征；根据所述测试特征得到对应的目标测试用例；根据所述目标测试用例对对应的目标待测装置集合中的待测装置进行漏洞测试。

[0006] 在其中一个实施例中，所述漏洞对应的测试特征包括所述漏洞所在的当前代码对应的代码特征，所述根据所述测试特征得到对应的目标测试用例的步骤包括：根据所述代码特征得到对应的目标测试用例。

[0007] 在其中一个实施例中，所述漏洞测试用例包括白盒测试用例，所述代码特征包括所述当前代码对应的控件标识，所述根据所述代码特征得到对应的目标测试用例的步骤包括：根据所述控件标识以及所述白盒测试用例的测试参数构造黑盒测试用例，作为目标测试用例。

[0008] 在其中一个实施例中，所述漏洞测试用例包括白盒测试用例，所述代码特征包括所述当前代码对应的变量约束条件以及所述当前代码对应的控件标识，所述根据所述代码

特征得到对应的目标测试用例的步骤包括：根据所述控件标识以及所述变量约束条件构造黑盒测试用例，作为目标测试用例。

[0009] 在其中一个实施例中，所述方法还包括：获取所述当前待测装置集合中各个待测装置的漏洞的危险度；根据所述各个漏洞的危险度以及对应的待测装置的重要度得到所述当前待测装置集合的安全风险，所述安全风险与所述危险度呈正相关关系，所述安全风险与所述重要度呈正相关关系。

[0010] 在其中一个实施例中，所述目标特征包括域名特征，所述获取所述当前待测装置集合中各个待测装置的目标特征，将具有相同目标特征的待测装置进行组合，得到所述各个目标特征对应的目标待测装置集合的步骤包括：获取所述当前待测装置集合中各个待测装置的域名，对所述各个待测装置的域名的无效信息进行过滤，得到域名特征；将具有相同域名特征的待测装置进行组合，得到相同的域名特征对应的目标待测装置集合。

[0011] 一种漏洞测试装置，所述装置包括：当前集合获取模块，用于获取待进行漏洞测试的当前待测装置集合，所述当前待测装置集合包括多个待测装置；组合模块，用于获取所述当前待测装置集合中各个待测装置的目标特征，将具有相同目标特征的待测装置进行组合，得到所述各个目标特征对应的目标待测装置集合；选取模块，用于从所述各个目标待测装置集合中分别选取至少一个测试装置，所述测试装置的数量小于对应的目标测试集合中全部待测装置的数量；测试装置测试模块，用于获取所述各个目标特征对应的漏洞测试用例，根据所述目标特征对应的漏洞测试用例对对应的测试装置进行漏洞测试，得到漏洞测试结果；待测装置测试模块，用于若所述漏洞测试结果为所述测试装置存在漏洞，根据所述漏洞对对应的目标待测装置集合中的待测装置进行漏洞测试。

[0012] 在其中一个实施例中，所述待测装置测试模块包括：测试特征得到单元，用于若所述漏洞测试结果为所述测试装置存在漏洞，获取所述漏洞对应的测试特征；目标测试用例得到单元，用于根据所述测试特征得到对应的目标测试用例；待测装置测试单元，用于根据所述目标测试用例对对应的目标待测装置集合中的待测装置进行漏洞测试。

[0013] 在其中一个实施例中，所述漏洞对应的测试特征包括所述漏洞所在的当前代码对应的代码特征，所述目标测试用例得到单元用于：根据所述代码特征得到对应的目标测试用例。

[0014] 在其中一个实施例中，所述漏洞测试用例包括白盒测试用例，所述代码特征包括所述当前代码对应的控件标识，所述目标测试用例得到单元用于：根据所述控件标识以及所述白盒测试用例的测试参数构造黑盒测试用例，作为目标测试用例。

[0015] 在其中一个实施例中，所述漏洞测试用例包括白盒测试用例，所述代码特征包括所述当前代码对应的变量约束条件以及所述当前代码对应的控件标识，所述目标测试用例得到单元用于：根据所述控件标识以及所述变量约束条件构造黑盒测试用例，作为目标测试用例。

[0016] 在其中一个实施例中，所述装置还包括：危险度获取模块，用于获取所述当前待测装置集合中各个待测装置的漏洞的危险度；风险得到模块，用于根据所述各个漏洞的危险度以及对应的待测装置的重要度得到所述当前待测装置集合的安全风险，所述安全风险与所述危险度呈正相关关系，所述安全风险与所述重要度呈正相关关系。

[0017] 在其中一个实施例中，所述目标特征包括域名特征，所述组合模块包括：域名获取

单元，用于获取所述当前待测装置集合中各个待测装置的域名，对所述各个待测装置的域名的无效信息进行过滤，得到域名特征；组合单元，用于将具有相同域名特征的待测装置进行组合，得到相同的域名特征对应的目标待测装置集合。

[0018] 一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现以下步骤：获取待进行漏洞测试的当前待测装置集合，所述当前待测装置集合包括多个待测装置；获取所述当前待测装置集合中各个待测装置的目标特征，将具有相同目标特征的待测装置进行组合，得到所述各个目标特征对应的目标待测装置集合；从所述各个目标待测装置集合中分别选取至少一个测试装置，所述测试装置的数量小于对应的目标测试集合中全部待测装置的数量；获取所述各个目标特征对应的漏洞测试用例，根据所述目标特征对应的漏洞测试用例对对应的测试装置进行漏洞测试，得到漏洞测试结果；若所述漏洞测试结果为所述测试装置存在漏洞，根据所述漏洞对对应的目标待测装置集合中的待测装置进行漏洞测试。

[0019] 一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现以下步骤：获取待进行漏洞测试的当前待测装置集合，所述当前待测装置集合包括多个待测装置；获取所述当前待测装置集合中各个待测装置的目标特征，将具有相同目标特征的待测装置进行组合，得到所述各个目标特征对应的目标待测装置集合；从所述各个目标待测装置集合中分别选取至少一个测试装置，所述测试装置的数量小于对应的目标测试集合中全部待测装置的数量；获取所述各个目标特征对应的漏洞测试用例，根据所述目标特征对应的漏洞测试用例对对应的测试装置进行漏洞测试，得到漏洞测试结果；若所述漏洞测试结果为所述测试装置存在漏洞，根据所述漏洞对对应的目标待测装置集合中的待测装置进行漏洞测试。

[0020] 上述漏洞测试方法、装置、计算机设备和存储介质，在需要进行漏洞测试时，获取待进行漏洞测试的当前待测装置集合，当前待测装置集合包括多个待测装置，获取当前待测装置集合中各个待测装置的目标特征，将具有相同目标特征的待测装置进行组合，得到各个目标特征对应的目标待测装置集合，从目标待测装置集合中选取对应的测试装置，获取漏洞测试用例，根据漏洞测试用例对测试装置进行漏洞测试，得到漏洞测试结果，若漏洞测试结果为测试装置存在漏洞，对目标待测装置集合对应的待测装置进行漏洞测试。由于在进行漏洞测试时，首先从具有相同目标特征的目标待测装置集合中选取测试设备进行测试，测试装置的数量小于目标测试集合待测装置的数量，当测试存在漏洞时对目标待测装置集合中对应的待测装置进行漏洞测试，因此可以减少在各个待测装置进行漏洞测试的测试用例的数量，提高了漏洞测试效率。

附图说明

[0021] 图1为一个实施例中漏洞测试方法的应用场景图；

[0022] 图2为一个实施例中漏洞测试方法的流程示意图；

[0023] 图3为一个实施例中若漏洞测试结果为测试装置存在漏洞，根据漏洞对对应的目标待测装置集合中的待测装置进行漏洞测试步骤的流程示意图；

[0024] 图4为一个实施例中漏洞测试方法的流程示意图；

[0025] 图5为一个实施例中获取当前待测装置集合中各个待测装置的目标特征，将具有

相同目标特征的待测装置进行组合，得到各个目标特征对应的目标待测装置集合步骤的流程示意图；

[0026] 图6为一个实施例中漏洞测试装置的结构框图；

[0027] 图7为一个实施例中待测装置测试模块的结构框图；

[0028] 图8为一个实施例中漏洞测试装置的结构框图；

[0029] 图9为一个实施例中组合模块的结构框图；

[0030] 图10为一个实施例中计算机设备的内部结构图。

具体实施方式

[0031] 为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本申请进行进一步详细说明。应当理解，此处描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。

[0032] 本申请提供的漏洞测试方法，可以应用于如图1所示的应用环境中。以当前待测设备集合包括三个待测装置104A、104B、104C，进行漏洞测试的为终端102为例。其中，终端102可以与当前待测设备集合的待测设备进行通信，例如可以是通过网络进行通信。终端102获取需要进行漏洞测试的当前待测装置集合，执行本发明实施例提供的漏洞测试方法进行测试，以提高漏洞测试效率。其中待测装置可以但不限于是各种个人计算机、笔记本电脑、智能手机、平板电脑、便携式可穿戴设备以及服务器等。可以理解，也可以将应用程序作为待测装置。此外，执行本发明实施例提供的漏洞测试方法的也可以服务器等。

[0033] 在一个实施例中，如图2所示，提供了一种漏洞测试方法，以执行该漏洞测试方法为图1中的终端为例进行说明，包括以下步骤：

[0034] 步骤S202，获取待进行漏洞测试的当前待测装置集合，当前待测装置集合包括多个待测装置。

[0035] 具体地，当前待测装置集合可以是预先设置的，例如已经预先设置了金融业务对应的设备作为当前待测装置集合。在一个实施例中，也可以利用装置探测工具对设备进行探测，得到当前待测装置集合。例如，向预设IP段的设备发送通信数据包，根据返回的通信数据包确定预设IP段内存活的设备，将存活的设备组成当前待测装置集合。当前待测装置集合的中待测装置的个数为多个，具体数量可以根据实际情况确定。例如可以是固定的个数，可以是根据业务平台中存活的计算机设备确定，也可以由测试人员根据需要进行选择。

[0036] 步骤S204，获取当前待测装置集合中各个待测装置的目标特征，将具有相同目标特征的待测装置进行组合，得到各个目标特征对应的目标待测装置集合。

[0037] 具体地，待测装置的目标特征可以是待测装置的操作系统、操作系统的版本、在业务平台上具有的功能、装置上应用所使用的程序语言、装置开放的端口以及域名等特征，具体可以根据需要进行设置。待测装置的目标特征可以是预先获取的。可以利用指纹探测工具确定待测装置的目标特征。例如可以利用whatweb工具构造获取特征的HTTP请求与待测装置进行交互，得到待测装置返回的响应包，根据响应包中的信息得到目标特征。得到待测装置的目标特征后，将具有相同目标特征的待测装置进行组合，得到目标特征所对应的目标待测装置集合。举个例子，假设有三个计算机设备为待测装置，A设备对应的目标特征为a、b以及c，B设备对应的目标特征为a、b，C设备对应的目标特征为a、c。则目标特征a对应的

目标待测装置集合包括A设备、B设备以及C设备，目标特征b对应的目标待测装置集合包括A设备以及B设备，目标特征c对应的目标待测装置集合包括A设备以及C设备。

[0038] 步骤S206，从所述各个目标待测装置集合中分别选取至少一个测试装置，所述测试装置的数量小于对应的目标测试集合中全部待测装置的数量。

[0039] 具体地，对于具有相同目标特征的目标待测装置集合，从中选择部分待测装置作为测试装置，即测试装置的数量小于该目标测试集合全部待测装置的数量。选择的测试装置的个数可以为一个或多个。例如，对于目标特征a对应的目标待测装置集合，可以选择A设备以及C设备作为待测装置，对于目标特征b对应的目标待测装置集合，可以选择B设备作为测试装置。对于目标特征C对应的目标待测装置集合，可以选择C设备作为测试装置。

[0040] 步骤S208，获取所述各个目标特征对应的漏洞测试用例，根据所述目标特征对应的漏洞测试用例对对应的测试装置进行漏洞测试，得到漏洞测试结果。

[0041] 具体地，设置了目标特征与漏洞测试用例的对应关系，对应关系具体可以根据需要进行设置。例如，对于具有XP操作系统且符合UPnP(Universal Plug and Play、通用即插即用)协议的特征的计算机设备，对应的测试用例可以包括对账号锁定功能进行测试的漏洞。测试用例可以是预先设置的。因此，根据目标特征得到漏洞测试用例后，将漏洞测试用例发送到该目标特征所对应的目标待测装置集合中选取的测试装置，以进行漏洞测试，得到漏洞测试结果。漏洞测试结果为存在漏洞或者不存在漏洞。可以理解，目标特征对应的漏洞测试用例可以有一个或多个。漏洞测试用例可以包括黑盒测试对应的测试用例以及白盒测试对应的测试用例中的一个或者组合。

[0042] 例如，对于目标特征a对应的目标待测装置集合，可以选择A设备以及C设备作为待测装置，对于目标特征b对应的目标待测装置集合，可以选择B设备作为测试装置。对于目标特征C对应的目标待测装置集合，可以选择C设备作为测试装置。因此，可以将目标特征a对应的漏洞测试用例发送给A设备以及C设备，将目标特征b对应的漏洞测试用例发送给B设备。将目标特征c对应的漏洞测试用例发送给C设备。

[0043] 步骤S210，若所述漏洞测试结果为所述测试装置存在漏洞，根据所述漏洞对对应的目标待测装置集合中的待测装置进行漏洞测试。

[0044] 具体地，当检测到漏洞后，可以获取漏洞所对应的测试用例对测试装置存在漏洞的目标待测装置集合中除测试装置外的待测装置进行漏洞测试。也可以根据漏洞相关的特征对测试装置存在漏洞的目标待测装置集合的部分或者全部待测装置进行漏洞测试。例如，可以获取与漏洞相关的代码的变量约束条件、漏洞对应代码的功能、漏洞所在的代码对应的控件标识中的一个或多个与漏洞相关的代码特征，根据代码特征获取对应的测试用例对目标待测装置集合对应的待测装置进行漏洞测试。

[0045] 在一个实施例中，漏洞测试用例包括白盒测试用例，可以先进行白盒测试，在漏洞测试过程中对白盒测试用例对应的代码进行扫描，得到代码中变量约束条件对应的代码语句。若存在漏洞，可以获取该漏洞所对应的代码中的变量约束条件，然后根据变量约束条件得到对应的黑盒测试中测试用例的参数，以构造黑盒测试用例，根据黑盒测试用例对目标待测装置集合对应的待测装置进行漏洞测试。变量约束条件是指当前代码中对输入的变量进行限制的限制条件。

[0046] 在一个实施例中，可以构造变量约束条件的边界值作为测试参数。例如，若代码中

变量约束条件为x大于5，则可以构造边界值5附近的参数作为黑盒的测试参数，如5.1、4.9999999999等。

[0047] 在一个实施例中，当变量约束条件包括两个以上时，则可以根据各个变量约束条件构造测试参数，再将各个变量约束条件的测试参数进行组合，得到最终的测试参数。例如登录密码的变量约束条件包括两个：大于10个字符以及首字符为数字。则可以根据大于10个字符的变量约束条件构造大于10个字符的有效测试参数、小于等于10个字符的无效测试参数。以及根据首字符为数字的变量约束条件构造首字母为数字的有效测试参数、首字符为非数字的无效测试参数。然后将根据变量约束条件构造的测试参数进行两两组合，得到黑盒的测试参数，假设构造的小于10个字符的测试参数为1001，首字符为数字的测试参数为a，则组合后最终得到的测试参数为a1001。

[0048] 在一个实施例中，当进行白盒测试时中发现漏洞，可以根据漏洞所对应的白盒测试用例的测试参数构造黑盒测试用例中的测试参数，如将白盒的测试用例的参数作为黑盒的测试参数，或者将白盒的测试参数进行变形后得到黑盒的测试参数。例如，若在白盒测试中测试参数为用户名“admin”，且利用该用户名进行登录时存在漏洞。则可以将admin、admin1作为黑盒测试用例的测试参数。

[0049] 在一个实施例中，白盒测试用例与黑盒测试用例的对应关系可以是预先设置的，可以根据白盒测试用例获取对应的黑盒测试用例。

[0050] 在一些实施例中，可以设置黑盒的测试用例与代码功能的对应关系，因此在进行白盒测试时，获取白盒测试用例对应的代码对应的控件，然后根据控件的功能描述得到对应的代码功能，进而得到对应的黑盒测试用例。控件的功能描述可以是预先设置的。

[0051] 在一个实施例中，在根据漏洞测试用例进行测试时，可以获取测试用例所对应的代码中开放的端口，向目标待测装置集合中的待测装置发送与开放的端口对应的测试用例。

[0052] 上述漏洞测试方法中，在需要进行漏洞测试时，获取待进行漏洞测试的当前待测装置集合，待测装置集合包括多个待测装置，获取当前待测装置集合中各个待测装置的目标特征，将具有相同目标特征的待测装置进行组合，得到各个目标特征对应的目标待测装置集合，从目标待测装置集合中选取对应的测试装置，获取漏洞测试用例，根据漏洞测试用例对测试装置进行漏洞测试，得到漏洞测试结果，若漏洞测试结果为测试装置存在漏洞，对目标待测装置集合对应的待测装置进行漏洞测试。由于在进行漏洞测试时，首先从具有相同目标特征的目标待测装置集合中选取测试设备进行测试，当测试存在漏洞时对目标待测装置集合中对应的待测装置进行漏洞测试，因此可以减少在各个待测装置进行漏洞测试的测试用例的数量，提高了漏洞测试效率。

[0053] 如图3所示，在一个实施例中，步骤S210即若所述漏洞测试结果为所述测试装置存在漏洞，根据所述漏洞对对应的目标待测装置集合中的待测装置进行漏洞测试的步骤包括：

[0054] 步骤S302，若漏洞测试结果为测试装置存在漏洞，获取漏洞对应的测试特征。

[0055] 具体地，漏洞对应的测试特征指与漏洞有关的特征。例如可以检测出漏洞的漏洞测试用例，检测出漏洞的漏洞测试用例的测试参数或者是漏洞对应的代码特征。漏洞对应的代码是指发现漏洞的代码。代码可以是一个代码段或代码块。代码特征可以包括代码对

应的变量约束条件和/或代码所对应的控件标识等。

[0056] 步骤S304，根据测试特征得到对应的目标测试用例。

[0057] 具体地，得到测试特征后，利用测试特征得到对应的目标测试用例。例如，可以根据测试变量条件构造测试用例的测试参数，若代码中变量约束条件为x大于10，则可以构造边界值附近的参数如9.9、10.1作为测试参数。然后将构造的测试参数替换原漏洞测试用例中的参数，形成目标测试用例。或者可以根据漏洞对应代码的功能获取对应的控件，然后构造触发该控件的测试用例，触发该控件的测试用例中的测试参数可以是漏洞测试用例中的测试参数。

[0058] 在一个实施例中，漏洞测试用例包括白盒测试用例，代码特征包括当前代码对应的控件标识，因此根据代码特征得到对应的目标测试用例的步骤包括：根据控件标识以及白盒测试用例的测试参数构造黑盒测试用例，作为目标测试用例。

[0059] 具体地，代码对应的控件标识可以是对代码进行检测得到的，也可以是预先设置的。得到控件标识后，根据白盒测试用例中的测试参数构造黑盒测试用例的测试参数，并构造触发控件标识对应控件以发送测试参数进行测试的黑盒测试用例，以模拟用户输入测试参数并触发控件进行漏洞测试的动作，对待测装置进行漏洞测试。例如，若在白盒测试中测试参数为用户名“admin”，且利用该用户名进行登录时存在漏洞。则可以将admin、admin1作为黑盒测试用例的测试参数。

[0060] 在一个实施例中，漏洞测试用例包括白盒测试用例，代码特征包括当前代码对应的变量约束条件以及当前代码对应的控件标识，因此因此根据代码特征得到对应的目标测试用例的步骤包括：根据控件标识以及变量约束条件构造黑盒测试用例，作为目标测试用例。

[0061] 具体地，代码对应的控件标识可以是对代码进行检测得到的，也可以是预先设置的。得到控件标识后，根据变量约束条件构造黑盒测试用例的测试参数，并构造控件标识对应的黑盒测试用例，以模拟输入黑盒测试用例的测试参数并触发控件的动作，对待测装置进行漏洞测试。例如若代码中变量约束条件为x大于10，则可以构造大于5的参数作为黑盒的测试参数，如5.1、190000000等。

[0062] 步骤S306，根据目标测试用例对对应的目标待测装置集合中的待测装置进行漏洞测试。

[0063] 具体地，得到目标测试测试用例后，可以向对应的目标待测装置集合的待测装置发送目标测试用例，以对目标待测装置集合对应的待测装置进行漏洞测试。

[0064] 在一个实施例中，如图4所示，漏洞测试方法还包括：

[0065] 步骤S402，获取当前待测装置集合中各个待测装置的漏洞的危险度。

[0066] 具体地，漏洞的危险度表示漏洞的危险程度，级别越高，则越危险。可以用数值表示例如90分、80分等。也可以用等级进行表示，例如高、中、低等。漏洞的危险度可以预先设置。当对当前目标待测集合的漏洞测试完成后，获取检测到的漏洞对应的危险度。

[0067] 步骤S404，根据各个漏洞的危险度以及对应的待测装置的重要度得到当前待测装置集合的安全风险。

[0068] 具体地，安全风险可以用数值表示，也可以用等级进行表示。重要度表示待测装置的重要程度，重要度越高，则越重要。重要度可以用数值表示，也可以用等级进行表示，例如

高、中、低等。待测装置的重要度可以是预先设置的。可以根据待测装置的所承担的功能确定，例如可以设置功能与重要度的对应关系。在一个实施例中，可以根据待测装置开放的端口得到对应的功能。例如，若待测装置开放的是80端口，则认为该待测装置在业务系统中承担服务器功能，重要度高。若计算机设备开放的是306端口，则认为待测装置在业务系统中承担数据库功能，重要度比服务器功能较低。根据各个漏洞的危险度及对应的待测装置的重要度得到当前待测装置集合的安全风险的方法可以根据实际需要进行设置。其中，安全风险与危险度呈正相关关系，安全风险与重要度呈正相关关系。例如，可以将危险分、重要分以及当前待测装置集合中该漏洞的个数进行相乘，得到该漏洞对应的分数，将当前待测装置集合中各个漏洞的分数进行求和得到当前待测装置集合的风险评分。结合漏洞的危险度以及对应的待测装置的重要度得到当前待测装置集合的安全风险能够展现当前待测装置集合的风险，以方便测试人员了解当前待测装置集合的危险情况。例如，若是对业务例如保险业务对应的计算机设备集合进行漏洞测试，则可以得到该保险业务整体的风险情况。

[0069] 在一个实施例中，目标特征包括域名特征，如图5所示，步骤S204即获取当前待测装置集合中各个待测装置的目标特征，将具有相同目标特征的待测装置进行组合，得到各个目标特征对应的目标待测装置集合的步骤包括：

[0070] 步骤S502，获取当前待测装置集合中各个待测装置的域名，对各个待测装置的域名的无效信息进行过滤，得到域名特征。

[0071] 具体地，域名的无效信息可以是预先设置的，具体可以根据需要进行设置。过滤是指去除无效信息，对于域名“http://www.test.com/login”，“http://”以及“/login”是无效信息。对于域名“https://www.baidu.com”、“https://www.baidu.cn”，“com”、“cn”是无效信息。对无效信息进行过滤后，得到域名特征。例如，http://ww.test.com/login”的域名特征是www.test.com。

[0072] 步骤S504，将具有相同域名特征的待测装置进行组合，得到相同的域名特征对应的目标待测装置集合。

[0073] 具体地，得到各个待测装置的的域名特征后，对待测装置的域名特征进行匹配，将具有相同域名特征的待测装置进行组合，得到相同的域名特征对应的目标待测集合。例如若A待测装置对应的域名为“https://www.baidu.com”，B待测装置对应的域名为“https://www.baidu.cn”，去除无效的信息“com”、“cn”后，域名特征相同，故可以将A待测装置以及B待测装置组合成目标待测装置集合。由于域名特征相同的待测装置很大可能都是由相同的团队设计以及编写代码的，可能具有相同的漏洞。因此若发现A待测装置检测到了漏洞，则可以对域名特征与A待测装置相同的B待测装置进行漏洞检测，提高测试效率。

[0074] 在一个实施例中，可以将域名相似的待测装置作为具有相同特征的待测装置。在获取待测装置的域名时，可以根据待测装置的外网IP地址得到待测装置的域名，然后对待测装置的域名进行对比，找出相似度大的域名，然后将域名相似度大的待测装置的内网IP地址进行关联。因此，若发现待测装置存在漏洞时，获取其关联的另一个待测装置的内网IP地址，根据内网IP地址向待测装置发送漏洞测试用例。域名是否相似的方法根据需要进行设置。例如，可以是主域名相同则为相似。

[0075] 应该理解的是，虽然上述的流程图中的各个步骤按照箭头的指示依次显示，但是这些步骤并不是必然按照箭头指示的顺序依次执行。除非本文中有明确的说明，这些步骤

的执行并没有严格的顺序限制，这些步骤可以以其它的顺序执行。而且，上述中的至少一部分步骤可以包括多个子步骤或者多个阶段，这些子步骤或者阶段并不必然是在同一时刻执行完成，而是可以在不同的时刻执行，这些子步骤或者阶段的执行顺序也不必然是依次进行，而是可以与其它步骤或者其它步骤的子步骤或者阶段的至少一部分轮流或者交替地执行。

[0076] 在一个实施例中，如图6所示，提供了一种漏洞测试装置，包括：当前集合获取模块602、组合模块604、选取模块606、测试装置测试模块608和待测装置测试模块610，其中：

[0077] 当前集合获取模块602，用于获取待进行漏洞测试的当前待测装置集合，当前待测装置集合包括多个待测装置。

[0078] 组合模块604，用于获取当前待测装置集合中各个待测装置的目标特征，将具有相同目标特征的待测装置进行组合，得到各个目标特征对应的目标待测装置集合。

[0079] 选取模块606，用于从所述各个目标待测装置集合中分别选取至少一个测试装置，所述测试装置的数量小于对应的目标测试集合中全部待测装置的数量。

[0080] 测试装置测试模块608，用于获取所述各个目标特征对应的漏洞测试用例，根据所述目标特征对应的漏洞测试用例对对应的测试装置进行漏洞测试，得到漏洞测试结果。

[0081] 待测装置测试模块610，用于若所述漏洞测试结果为所述测试装置存在漏洞，根据所述漏洞对对应的目标待测装置集合中的待测装置进行漏洞测试。

[0082] 在其中一个实施例中，如图7所示，待测装置测试模块610包括：

[0083] 测试特征得到单元610A，用于若漏洞测试结果为测试装置存在漏洞，获取漏洞对应的测试特征。

[0084] 目标测试用例得到单元610B，用于根据测试特征得到对应的目标测试用例。

[0085] 待测装置测试单元610C，用于根据目标测试用例对对应的目标待测装置集合中的待测装置进行漏洞测试。

[0086] 在其中一个实施例中，漏洞对应的测试特征包括漏洞所在的当前代码对应的代码特征，目标测试用例得到单元610B用于：根据代码特征得到对应的目标测试用例。

[0087] 在其中一个实施例中，漏洞测试用例包括白盒测试用例，代码特征包括当前代码对应的控件标识，目标测试用例得到单元610B用于：根据控件标识以及白盒测试用例的测试参数构造黑盒测试用例，作为目标测试用例。

[0088] 在其中一个实施例中，漏洞测试用例包括白盒测试用例，代码特征包括当前代码对应的变量约束条件以及当前代码对应的控件标识，目标测试用例得到单元610B用于：根据控件标识以及变量约束条件构造黑盒测试用例，作为目标测试用例。

[0089] 在其中一个实施例中，如图8所示，漏洞检测装置还包括：

[0090] 危险度获取模块802，用于获取当前待测装置集合中各个待测装置的漏洞的危险度。

[0091] 风险得到模块804，用于根据各个漏洞的危险度以及对应的待测装置的重要度得到当前待测装置集合的安全风险，安全风险与危险度呈正相关关系，安全风险与重要度呈正相关关系。

[0092] 在其中一个实施例中，目标特征包括域名特征，如图9所示，组合模块604包括：

[0093] 域名获取单元604A，用于获取当前待测装置集合中各个待测装置的域名，对各个

待测装置的域名的无效信息进行过滤，得到域名特征。

[0094] 组合单元604B，用于将具有相同域名特征的待测装置进行组合，得到相同的域名特征对应的目标待测装置集合。

[0095] 关于漏洞测试装置的具体限定可以参见上文中对于漏洞测试方法的限定，在此不再赘述。上述漏洞测试装置中的各个模块可全部或部分通过软件、硬件及其组合来实现。上述各模块可以硬件形式内嵌于或独立于计算机设备中的处理器中，也可以以软件形式存储于计算机设备中的存储器中，以便于处理器调用执行以上各个模块对应的操作。

[0096] 在一个实施例中，提供了一种计算机设备，该计算机设备可以是服务器也可以是终端，其内部结构图可以如图10所示。该计算机设备包括通过系统总线连接的处理器、存储器和网络接口。其中，该计算机设备的处理器用于提供计算和控制能力。该计算机设备的存储器包括非易失性存储介质、内存储器。该非易失性存储介质存储有操作系统、计算机程序和数据库。该内存储器为非易失性存储介质中的操作系统和计算机程序的运行提供环境。该计算机设备的网络接口用于与外部的终端通过网络连接通信。该计算机程序被处理器执行时以实现一种漏洞检测方法。

[0097] 本领域技术人员可以理解，图10中示出的结构，仅仅是与本申请方案相关的部分结构的框图，并不构成对本申请方案所应用于其上的计算机设备的限定，具体的计算机设备可以包括比图中所示更多或更少的部件，或者组合某些部件，或者具有不同的部件布置。

[0098] 在一个实施例中，提供了一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，处理器执行计算机程序时实现以下步骤：获取待进行漏洞测试的当前待测装置集合，当前待测装置集合包括多个待测装置；获取当前待测装置集合中各个待测装置的目标特征，将具有相同目标特征的待测装置进行组合，得到各个目标特征对应的目标待测装置集合；从所述各个目标待测装置集合中分别选取至少一个测试装置，所述测试装置的数量小于对应的目标测试集合中全部待测装置的数量；获取所述各个目标特征对应的漏洞测试用例，根据所述目标特征对应的漏洞测试用例对对应的测试装置进行漏洞测试，得到漏洞测试结果；若所述漏洞测试结果为所述测试装置存在漏洞，根据所述漏洞对对应的目标待测装置集合中的待测装置进行漏洞测试。

[0099] 在其中一个实施例中，若漏洞测试结果为测试装置存在漏洞，处理器所执行的根据漏洞对目标待测装置集合对应的待测装置进行漏洞测试的步骤包括：若漏洞测试结果为测试装置存在漏洞，获取漏洞对应的测试特征；根据测试特征得到对应的目标测试用例；根据目标测试用例对对应的目标待测装置集合中的待测装置进行漏洞测试。

[0100] 在其中一个实施例中，漏洞对应的测试特征包括漏洞所在的当前代码对应的代码特征，处理器所执行的根据测试特征得到对应的目标测试用例的步骤包括：根据代码特征得到对应的目标测试用例。

[0101] 在其中一个实施例中，漏洞测试用例包括白盒测试用例，代码特征包括当前代码对应的控件标识，处理器所执行的根据代码特征得到对应的目标测试用例的步骤包括：根据控件标识以及白盒测试用例的测试参数构造黑盒测试用例，作为目标测试用例。

[0102] 在其中一个实施例中，漏洞测试用例包括白盒测试用例，代码特征包括当前代码对应的变量约束条件以及当前代码对应的控件标识，处理器所执行的根据代码特征得到对应的目标测试用例的步骤包括：根据控件标识以及变量约束条件构造黑盒测试用例，作为

目标测试用例。

[0103] 在其中一个实施例中，处理器执行计算机程序时还实现以下步骤：获取当前待测装置集合中各个待测装置的漏洞的危险度；根据各个漏洞的危险度以及对应的待测装置的重要度得到当前待测装置集合的安全风险，安全风险与危险度呈正相关关系，安全风险与重要度呈正相关关系。

[0104] 在其中一个实施例中，目标特征包括域名特征，获取当前待测装置集合中各个待测装置的目标特征，处理器所执行的将具有相同目标特征的待测装置进行组合，得到目标特征对应的目标待测装置集合的步骤包括：获取当前待测装置集合中各个待测装置的域名，对各个待测装置的域名的无效信息进行过滤，得到域名特征；将具有相同域名特征的待测装置进行组合，得到相同的域名特征对应的目标待测装置集合。

[0105] 在一个实施例中，提供了一种计算机可读存储介质，其上存储有计算机程序，计算机程序被处理器执行时实现以下步骤：获取待进行漏洞测试的当前待测装置集合，当前待测装置集合包括多个待测装置；获取当前待测装置集合中各个待测装置的目标特征，将具有相同目标特征的待测装置进行组合，得到各个目标特征对应的目标待测装置集合；从所述各个目标待测装置集合中分别选取至少一个测试装置，所述测试装置的数量小于对应的目标测试集合中全部待测装置的数量；获取所述各个目标特征对应的漏洞测试用例，根据所述目标特征对应的漏洞测试用例对对应的测试装置进行漏洞测试，得到漏洞测试结果；若所述漏洞测试结果为所述测试装置存在漏洞，根据所述漏洞对对应的目标待测装置集合中的待测装置进行漏洞测试。

[0106] 在其中一个实施例中，若漏洞测试结果为测试装置存在漏洞，处理器所执行的根据漏洞对目标待测装置集合对应的待测装置进行漏洞测试的步骤包括：若漏洞测试结果为测试装置存在漏洞，获取漏洞对应的测试特征；根据测试特征得到对应的目标测试用例；根据目标测试用例对对应的目标待测装置集合中的待测装置进行漏洞测试。

[0107] 在其中一个实施例中，漏洞对应的测试特征包括漏洞所在的当前代码对应的代码特征，处理器所执行的根据测试特征得到对应的目标测试用例的步骤包括：根据代码特征得到对应的目标测试用例。

[0108] 在其中一个实施例中，漏洞测试用例包括白盒测试用例，代码特征包括当前代码对应的控件标识，处理器所执行的根据代码特征得到对应的目标测试用例的步骤包括：根据控件标识以及白盒测试用例的测试参数构造黑盒测试用例，作为目标测试用例。

[0109] 在其中一个实施例中，漏洞测试用例包括白盒测试用例，代码特征包括当前代码对应的变量约束条件以及当前代码对应的控件标识，处理器所执行的根据代码特征得到对应的目标测试用例的步骤包括：根据控件标识以及变量约束条件构造黑盒测试用例，作为目标测试用例。

[0110] 在其中一个实施例中，处理器执行计算机程序时还实现以下步骤：获取当前待测装置集合中各个待测装置的漏洞的危险度；根据各个漏洞的危险度以及对应的待测装置的重要度得到当前待测装置集合的安全风险，安全风险与危险度呈正相关关系，安全风险与重要度呈正相关关系。

[0111] 在其中一个实施例中，目标特征包括域名特征，获取当前待测装置集合中各个待测装置的目标特征，处理器所执行的将具有相同目标特征的待测装置进行组合，得到目标

特征对应的目标待测装置集合的步骤包括:获取当前待测装置集合中各个待测装置的域名,对各个待测装置的域名的无效信息进行过滤,得到域名特征;将具有相同域名特征的待测装置进行组合,得到相同的域名特征对应的目标待测装置集合。

[0112] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程,是可以通过计算机程序来指令相关的硬件来完成,所述的计算机程序可存储于一非易失性计算机可读取存储介质中,该计算机程序在执行时,可包括如上述各方法的实施例的流程。其中,本申请所提供的各实施例中所使用的对存储器、存储、数据库或其它介质的任何引用,均可包括非易失性和/或易失性存储器。非易失性存储器可包括只读存储器(ROM)、可编程ROM(PROM)、电可编程ROM(EPROM)、电可擦除可编程ROM(EEPROM)或闪存。易失性存储器可包括随机存取存储器(RAM)或者外部高速缓冲存储器。作为说明而非局限,RAM以多种形式可得,诸如静态RAM(SRAM)、动态RAM(DRAM)、同步DRAM(SDRAM)、双数据率SDRAM(DDRSDRAM)、增强型SDRAM(ESDRAM)、同步链路(Synchlink)DRAM(SLDRAM)、存储器总线(Rambus)直接RAM(RDRAM)、直接存储器总线动态RAM(DRDRAM)、以及存储器总线动态RAM(RDRAM)等。

[0113] 以上实施例的各技术特征可以进行任意的组合,为使描述简洁,未对上述实施例中的各个技术特征所有可能的组合都进行描述,然而,只要这些技术特征的组合不存在矛盾,都应当认为是本说明书记载的范围。

[0114] 以上所述实施例仅表达了本申请的几种实施方式,其描述较为具体和详细,但并不能因此而理解为对发明专利范围的限制。应当指出的是,对于本领域的普通技术人员来说,在不脱离本申请构思的前提下,还可以做出若干变形和改进,这些都属于本申请的保护范围。因此,本申请专利的保护范围应以所附权利要求为准。

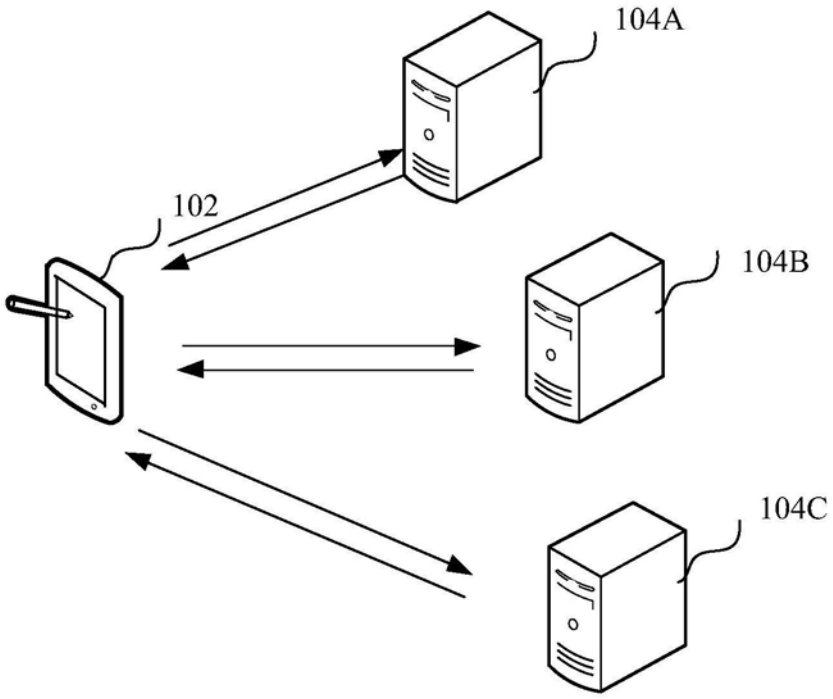


图1

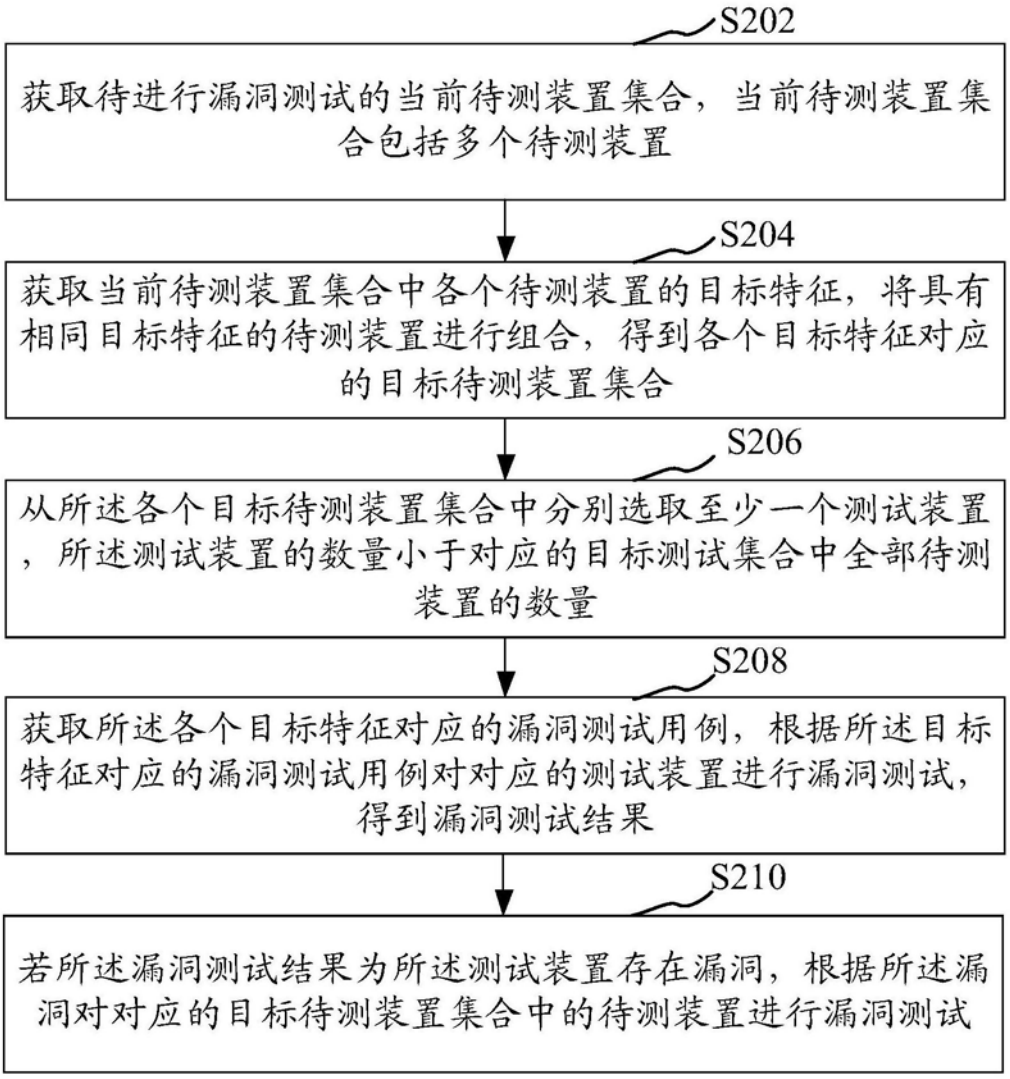

S202
获取待进行漏洞测试的当前待测装置集合，当前待测装置集合包括多个待测装置
S204
获取当前待测装置集合中各个待测装置的目标特征，将具有相同目标特征的待测装置进行组合，得到各个目标特征对应的目标待测装置集合
S206
从所述各个目标待测装置集合中分别选取至少一个测试装置，所述测试装置的数量小于对应的目标测试集合中全部待测装置的数量
S208
获取所述各个目标特征对应的漏洞测试用例，根据所述目标特征对应的漏洞测试用例对对应的测试装置进行漏洞测试，得到漏洞测试结果
S210
若所述漏洞测试结果为所述测试装置存在漏洞，根据所述漏洞对对应的目标待测装置集合中的待测装置进行漏洞测试

图2

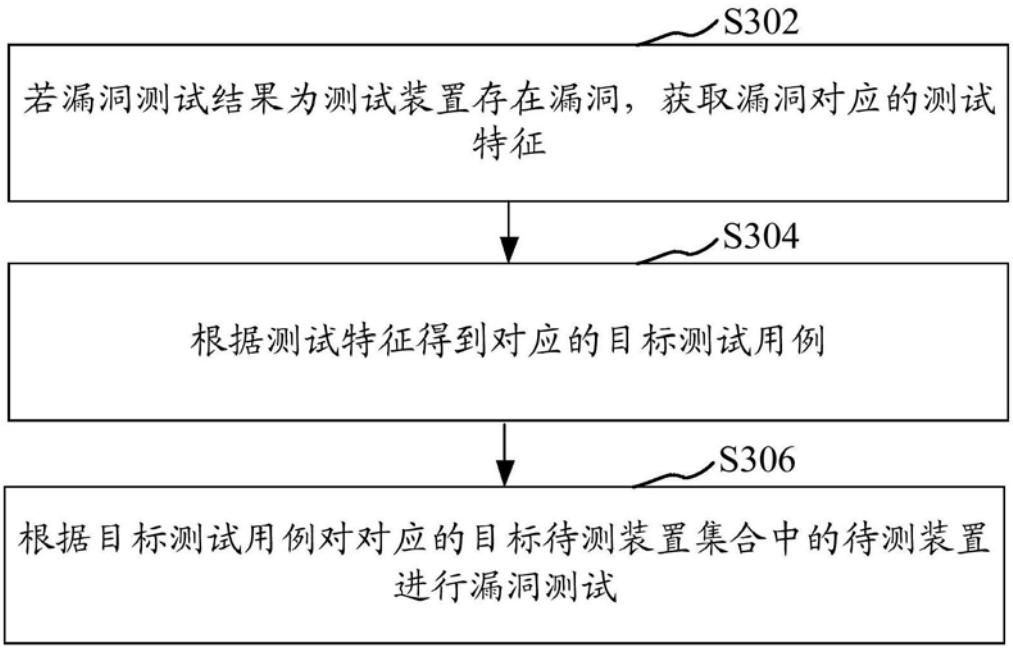

S302
若漏洞测试结果为测试装置存在漏洞，获取漏洞对应的测试特征
S304
根据测试特征得到对应的目标测试用例
S306
根据目标测试用例对对应的目标待测装置集合中的待测装置进行漏洞测试

图3

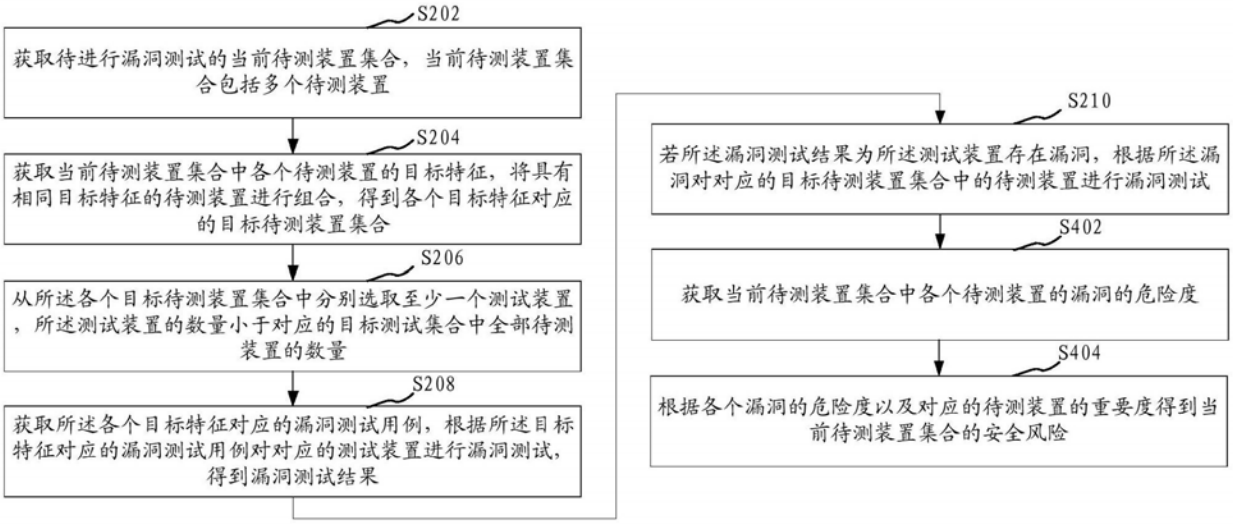

S202
获取待进行漏洞测试的当前待测装置集合，当前待测装置集合包括多个待测装置
S204
获取当前待测装置集合中各个待测装置的目标特征，将具有相同目标特征的待测装置进行组合，得到各个目标特征对应的目标待测装置集合
S206
从所述各个目标待测装置集合中分别选取至少一个测试装置，所述测试装置的数量小于对应的目标测试集合中全部待测装置的数量
S208
获取所述各个目标特征对应的漏洞测试用例，根据所述目标特征对应的漏洞测试用例对对应的测试装置进行漏洞测试，得到漏洞测试结果
S210
若所述漏洞测试结果为所述测试装置存在漏洞，根据所述漏洞对对应的目标待测装置集合中的待测装置进行漏洞测试
S402
获取当前待测装置集合中各个待测装置的漏洞的危险度
S404
根据各个漏洞的危险度以及对应的待测装置的重要度得到当前待测装置集合的安全风险

图4

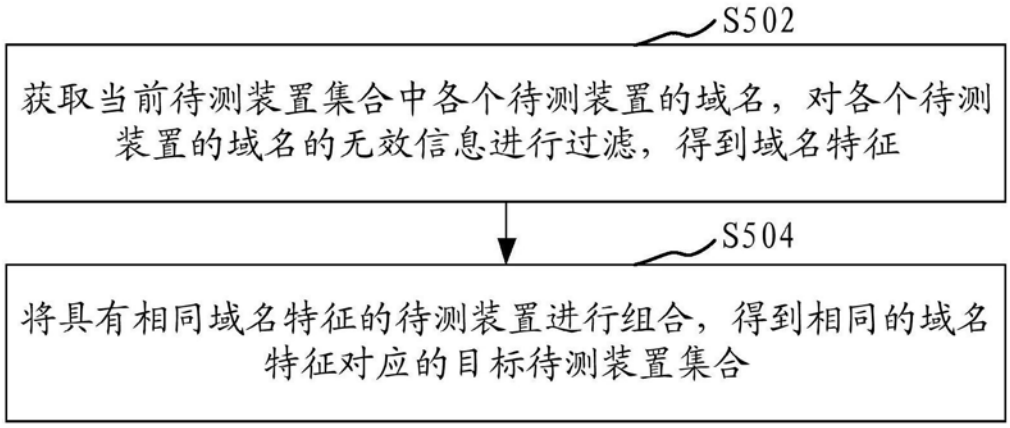

S502
获取当前待测装置集合中各个待测装置的域名，对各个待测装置的域名的无效信息进行过滤，得到域名特征
S504
将具有相同域名特征的待测装置进行组合，得到相同的域名特征对应的目标待测装置集合

图5

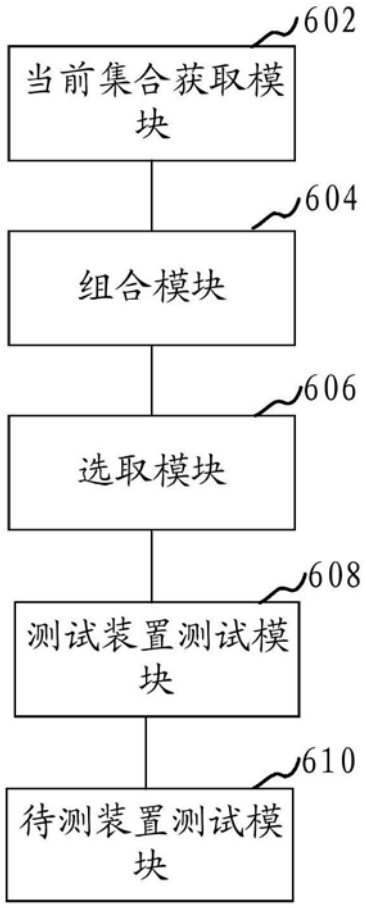

602
当前集合获取模块
604
组合模块
606
选取模块
608
测试装置测试模块
610
待测装置测试模块

图6

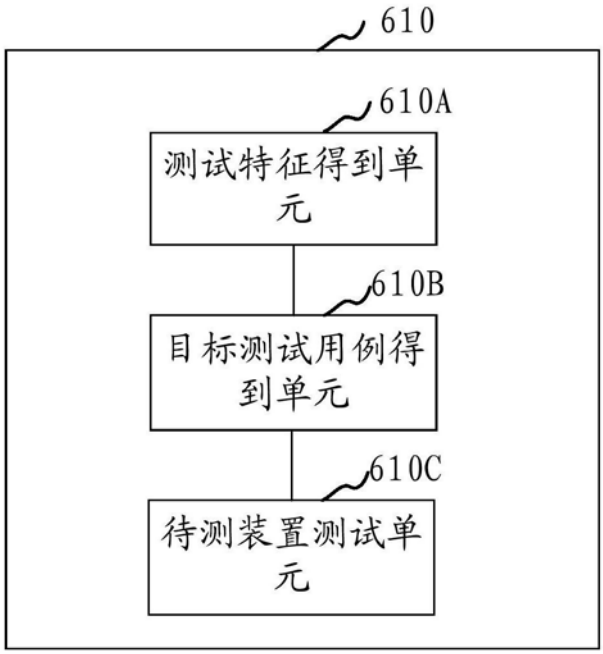

610
610A
测试特征得到单元
610B
目标测试用例得到单元
610C
待测装置测试单元

图7

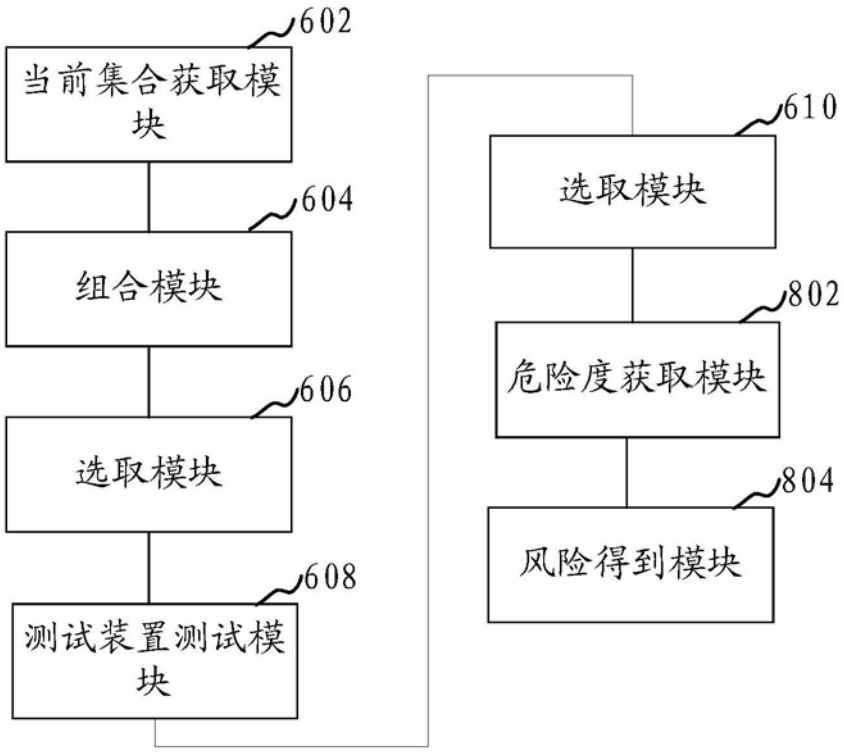

602
当前集合获取模块
604
组合模块
606
选取模块
608
测试装置测试模块
610
选取模块
802
危险度获取模块
804
风险得到模块

图8

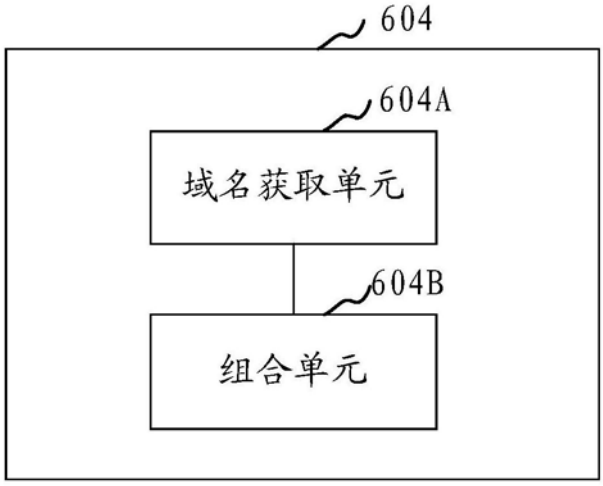

604
604A
域名获取单元
604B
组合单元

图9

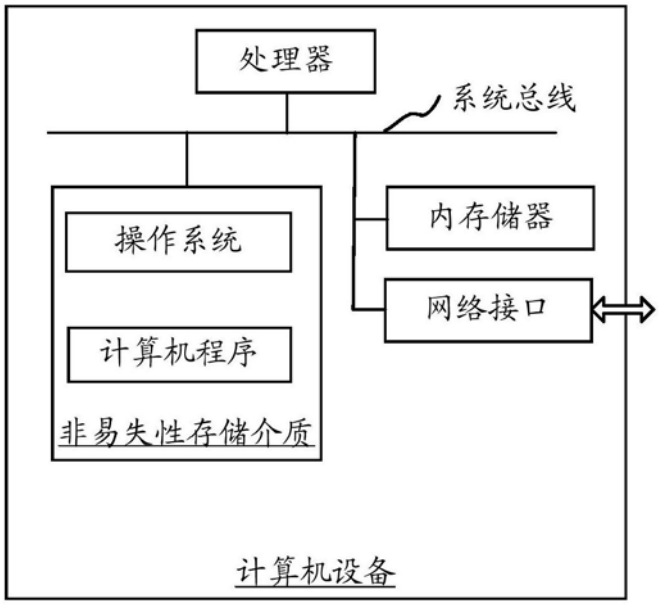

处理器
系统总线
操作系统
计算机程序
非易失性存储介质
内存储器
网络接口
计算机设备

图10