(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 111913877 A
(43)申请公布日 2020.11.10

(21)申请号 202010636048.7

(22)申请日 2020.07.03

(71)申请人 中国科学院信息工程研究所
地址 100093 北京市海淀区闵庄路甲89号

(72)发明人 宋站威 曾怡诚 刘明东 朱红松 李志 孙利民 石志强

(74)专利代理机构 北京路浩知识产权代理有限公司 11002
代理人 杨明月

(51)Int.Cl.
G06F 11/36(2006.01)

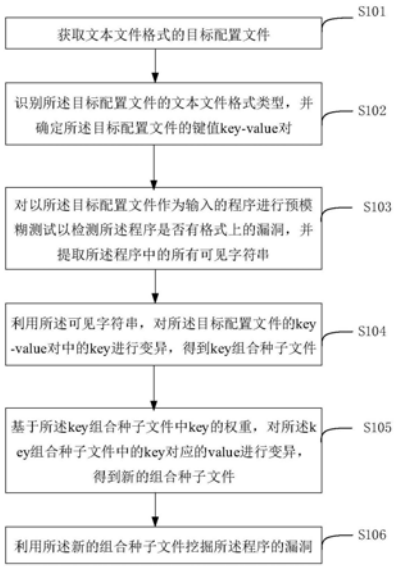
权利要求书2页 说明书9页 附图2页

(54)发明名称

一种面向文本配置文件的模糊测试方法及装置

(57)摘要

本发明实施例提供一种面向文本配置文件的模糊测试方法及装置,所述方法包括:识别所述目标配置文件的文本文件格式类型,并确定所述目标配置文件的键值key-value对;对以所述目标配置文件作为输入的程序进行预模糊测试以检测所述程序是否有格式上的漏洞,并提取所述程序中的所有可见字符串,对所述目标配置文件的key-value对中的key进行变异,得到key组合种子文件;基于所述key组合种子文件中key的权重,对所述key组合种子文件中的key对应的value进行变异,得到新的组合种子文件,挖掘所述程序的漏洞。本发明实施例实现了全面地挖掘程序中较深层次的漏洞,提升面向文本配置文件的模糊测试效率。



CN 111913877 A

1.一种面向文本配置文件的模糊测试方法,其特征在于,包括:

获取文本文件格式的目标配置文件;

识别所述目标配置文件的文本文件格式类型,并确定所述目标配置文件的键值key-value对;

对以所述目标配置文件作为输入的程序进行预模糊测试以检测所述程序是否有格式上的漏洞,并提取所述程序中的所有可见字符串;

利用所述可见字符串,对所述目标配置文件的key-value对中的key进行变异,得到key组合种子文件;

基于所述key组合种子文件中key的权重,对所述key组合种子文件中的key对应的value进行变异,得到新的组合种子文件;

利用所述新的组合种子文件挖掘所述程序的漏洞。

2.根据权利要求1所述的面向文本配置文件的模糊测试方法,其特征在于,所述利用所述可见字符串,对所述目标配置文件的key-value对中的key进行变异,得到key组合种子文件,具体包括:

针对每个所述可见字符串,利用当前可见字符串替换所述key-value对中的key,得到种子文件,将所述种子文件作为输入插桩执行,若产生了新的执行路径,则将所述key存储至有效key集合;

基于所述有效key集合,依次对所述种子文件中的key随机地进行删除、替换和增加操作中的任一种,得到key组合种子文件。

3.根据权利要求1所述的面向文本配置文件的模糊测试方法,其特征在于,所述基于所述key组合种子文件中key的权重,对所述key组合种子文件中的key对应的value进行变异,得到新的组合种子文件,具体包括:

针对所述key组合种子文件中的每个key对应的value进行变异,若判断插桩执行后产生了新的执行路径,根据所述新的执行路径中产生的新代码块数量设置对应key的权重;

从权重高的前N个key中随机选取M个key,对所述M个key对应的value进行变异,若判断插桩执行后产生了新的执行路径,则同时增大所述M个key的权重,或者,若判断插桩执行后没有产生新的执行路径,则同时减小所述M个key的权重,若所述M个key中存在P个key的权重低于权重高的前N个key的权重,则重新从权重高的前N个key中随机选取M个key,直至所述M个key的权重都不大于权重阈值,得到新的组合种子文件;

其中,N,M和P均为大于等于1的自然数,N≥M≥P。

4.根据权利要求1所述的面向文本配置文件的模糊测试方法,其特征在于,所述对所述key组合种子文件中的key对应的value进行变异,具体包括:

循环执行以下步骤预设次数:随机选择一条操作策略对所述key组合种子文件中的Q个key对应的value进行变异;

其中,所述预设次数根据所述key对应的value的数据长度确定;所述操作策略包括按位翻转,整数加减,数据插入和数据删减;Q为大于等于1的自然数。

5.一种面向文本配置文件的模糊测试装置,其特征在于,包括:

获取模块,用于获取文本文件格式的目标配置文件;

识别模块,用于识别所述目标配置文件的文本文件格式类型,并确定所述目标配置文

件的键值key-value对；

检测提取模块，用于对以所述目标配置文件作为输入的程序进行预模糊测试以检测所述程序是否有格式上的漏洞，并提取所述程序中的所有可见字符串；

key变异模块，用于利用所述可见字符串，对所述目标配置文件的key-value对中的key进行变异，得到key组合种子文件；

value变异模块，用于基于所述key组合种子文件中key的权重，对所述key组合种子文件中的key对应的value进行变异，得到新的组合种子文件；

挖掘模块，用于利用所述新的组合种子文件挖掘所述程序的漏洞。

6.根据权利要求5所述的面向文本配置文件的模糊测试装置，其特征在于，所述key变异模块，具体用于：

针对每个所述可见字符串，利用当前可见字符串替换所述key-value对中的key，得到种子文件，将所述种子文件作为输入插桩执行，若产生了新的执行路径，则将所述key存储至有效key集合；

基于所述有效key集合，依次对所述种子文件中的key随机地进行删除、替换和增加操作中的任一种，得到key组合种子文件。

7.根据权利要求5所述的面向文本配置文件的模糊测试装置，其特征在于，所述value变异模块，具体用于：

针对所述key组合种子文件中的每个key对应的value进行变异，若判断插桩执行后产生了新的执行路径，根据所述新的执行路径中产生的新代码块数量设置对应key的权重；

从权重高的前N个key中随机选取M个key，对所述M个key对应的value进行变异，若判断插桩执行后产生了新的执行路径，则同时增大所述M个key的权重，或者，若判断插桩执行后没有产生新的执行路径，则同时减小所述M个key的权重，若所述M个key中存在P个key的权重低于权重高的前N个key的权重，则重新从权重高的前N个key中随机选取M个key，直至所述M个key的权重都不大于权重阈值，得到新的组合种子文件；

其中，N,M和P均为大于等于1的自然数，N≥M≥P。

8.根据权利要求5所述的面向文本配置文件的模糊测试装置，其特征在于，所述value变异模块，具体还用于：

循环执行以下步骤预设次数：随机选择一条操作策略对所述key组合种子文件中的Q个key对应的value进行变异；

其中，所述预设次数根据所述key对应的value的数据长度确定；所述操作策略包括按位翻转，整数加减，数据插入和数据删减；Q为大于等于1的自然数。

9.一种电子设备，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程序时实现如权利要求1至4任一项所述的面向文本配置文件的模糊测试方法的步骤。

10.一种非暂态计算机可读存储介质，其上存储有计算机程序，其特征在于，该计算机程序被处理器执行时实现如权利要求1至4任一项所述的面向文本配置文件的模糊测试方法的步骤。

一种面向文本配置文件的模糊测试方法及装置

技术领域

[0001] 本发明涉及漏洞挖掘与分析领域，具体涉及一种面向文本配置文件的模糊测试方法及装置。

背景技术

[0002] 模糊测试是一项通过动态方式对软件或系统进行漏洞挖掘的技术。模糊测试工具以AFL为代表，其理念为动态执行与路径覆盖率提高，大致实现方式为将种子文件作为输入实际执行测试程序，同时通过插桩的方式记录每个种子文件对应的执行路径，随后对种子文件尝试变异，以尝试使得变异后的种子文件作为程序输入能够让程序经过不同的执行路径。

[0003] 在模糊测试的现有技术中，输入类型往往是多种多样的，可以是通过socket进行网络数据输入，也可以是对程序命令行参数读取输入，还有可能是直接从程序的配置文件中读取输入。但是同一个模糊测试方法，即变异算法，针对不同类型输入程序的模糊测试的效率和覆盖率不够高。

[0004] 因此，如何实现面向文本配置文件的模糊测试方法，提升面向文本配置文件的模糊测试效率和覆盖率，成为亟待解决的问题。

发明内容

[0005] 针对现有技术中的缺陷，本发明实施例提供一种面向文本配置文件的模糊测试方法及装置。

[0006] 第一方面，本发明实施例提供一种面向文本配置文件的模糊测试方法，包括：

[0007] 获取文本文件格式的目标配置文件；

[0008] 识别所述目标配置文件的文本文件格式类型，并确定所述目标配置文件的键值key-value对；

[0009] 对以所述目标配置文件作为输入的程序进行预模糊测试以检测所述程序是否有格式上的漏洞，并提取所述程序中的所有可见字符串；

[0010] 利用所述可见字符串，对所述目标配置文件的key-value对中的key进行变异，得到key组合种子文件；

[0011] 基于所述key组合种子文件中key的权重，对所述key组合种子文件中的key对应的value进行变异，得到新的组合种子文件；

[0012] 利用所述新的组合种子文件挖掘所述程序的漏洞。

[0013] 可选地，所述利用所述可见字符串，对所述目标配置文件的key-value对中的key进行变异，得到key组合种子文件，具体包括：

[0014] 针对每个所述可见字符串，利用当前可见字符串替换所述key-value对中的key，得到种子文件，将所述种子文件作为输入插桩执行，若产生了新的执行路径，则将所述key存储至有效key集合；

[0015] 基于所述有效key集合，依次对所述种子文件中的key随机地进行删除、替换和增加操作中的任一种，得到key组合种子文件。

[0016] 可选地，所述基于所述key组合种子文件中key的权重，对所述key组合种子文件中的key对应的value进行变异，得到新的组合种子文件，具体包括：

[0017] 针对所述key组合种子文件中的每个key对应的value进行变异，若判断插桩执行后产生了新的执行路径，根据所述新的执行路径中产生的新代码块数量设置对应key的权重；

[0018] 从权重高的前N个key中随机选取M个key，对所述M个key对应的value进行变异，若判断插桩执行后产生了新的执行路径，则同时增大所述M个key的权重，或者，若判断插桩执行后没有产生新的执行路径，则同时减小所述M个key的权重，若所述M个key中存在P个key的权重低于权重高的前N个key的权重，则重新从权重高的前N个key中随机选取M个key，直至所述M个key的权重都不大于权重阈值，得到新的组合种子文件；

[0019] 其中，N,M和P均为大于等于1的自然数，N≥M≥P。

[0020] 可选地，所述对所述key组合种子文件中的key对应的value进行变异，具体包括：

[0021] 循环执行以下步骤预设次数：随机选择一条操作策略对所述key组合种子文件中的Q个key对应的value进行变异；

[0022] 其中，所述预设次数根据所述key对应的value的数据长度确定；所述操作策略包括按位翻转，整数加减，数据插入和数据删减；Q为大于等于1的自然数。

[0023] 第二方面，本发明实施例提供一种面向文本配置文件的模糊测试装置，包括：

[0024] 获取模块，用于获取文本文件格式的目标配置文件；

[0025] 识别模块，用于识别所述目标配置文件的文本文件格式类型，并确定所述目标配置文件的键值key-value对；

[0026] 检测提取模块，用于对以所述目标配置文件作为输入的程序进行预模糊测试以检测所述程序是否有格式上的漏洞，并提取所述程序中的所有可见字符串；

[0027] key变异模块，用于利用所述可见字符串，对所述目标配置文件的key-value对中的key进行变异，得到key组合种子文件；

[0028] value变异模块，用于基于所述key组合种子文件中key的权重，对所述key组合种子文件中的key对应的value进行变异，得到新的组合种子文件；

[0029] 挖掘模块，用于利用所述新的组合种子文件挖掘所述程序的漏洞。

[0030] 可选地，所述时间窗口内的采样频率固定设置，且至少为肌电信号频率有效值的两倍。

[0031] 可选地，所述key变异模块，具体用于：

[0032] 针对每个所述可见字符串，利用当前可见字符串替换所述key-value对中的key，得到种子文件，将所述种子文件作为输入插桩执行，若产生了新的执行路径，则将所述key存储至有效key集合；

[0033] 基于所述有效key集合，依次对所述种子文件中的key随机地进行删除、替换和增加操作中的任一种，得到key组合种子文件。

[0034] 可选地，所述value变异模块，具体用于：

[0035] 针对所述key组合种子文件中的每个key对应的value进行变异，若判断插桩执行

后产生了新的执行路径，根据所述新的执行路径中产生的新代码块数量设置对应key的权重；

[0036] 从权重高的前N个key中随机选取M个key，对所述M个key对应的value进行变异，若判断插桩执行后产生了新的执行路径，则同时增大所述M个key的权重，或者，若判断插桩执行后没有产生新的执行路径，则同时减小所述M个key的权重，若所述M个key中存在P个key的权重低于权重高的前N个key的权重，则重新从权重高的前N个key中随机选取M个key，直至所述M个key的权重都不大于权重阈值，得到新的组合种子文件；

[0037] 其中，N，M和P均为大于等于1的自然数，N≥M≥P。

[0038] 可选地，所述value变异模块，具体还用于：

[0039] 循环执行以下步骤预设次数：随机选择一条操作策略对所述key组合种子文件中的Q个key对应的value进行变异；

[0040] 其中，所述预设次数根据所述key对应的value的数据长度确定；所述操作策略包括按位翻转，整数加减，数据插入和数据删减；Q为大于等于1的自然数。

[0041] 第三方面本发明实施例提供一种电子设备，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程序时实现以上第一方面所述的面向文本配置文件的模糊测试方法的步骤。

[0042] 第四方面本发明实施例提供一种非暂态计算机可读存储介质，其上存储有计算机程序，该计算机程序被处理器执行时实现以上第一方面所述的面向文本配置文件的模糊测试方法的步骤。

[0043] 本发明实施例提供了面向文本配置文件的模糊测试方法，该方法中，通过对以文本文件格式的目标配置文件作为输入的程序进行预模糊测试、key变异和value变异，得到新的组合种子文件，并进行模糊测试，能够全面地挖掘程序中较深层次的漏洞，提升面向文本配置文件的模糊测试效率。

附图说明

[0044] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0045] 图1为本发明实施例提供的一种面向文本配置文件的模糊测试方法的流程示意图；

[0046] 图2为本发明实施例提供的另一面向文本配置文件的模糊测试方法的流程示意图；

[0047] 图3为本发明实施例提供的面向文本配置文件的模糊测试装置的结构示意图；

[0048] 图4是本发明实施例提供的一种电子设备的实体结构示意图。

具体实施方式

[0049] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是

本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0050] 图1是本发明实施例提供的一种心电电极复用为按键的方法的流程示意图，图2是本发明实施例提供的另一心电电极复用为按键的方法的流程示意图，如图1和2所示，所述方法包括：

[0051] S101：获取文本文件格式的目标配置文件。

[0052] 其中，所述目标配置文件的格式一般包括二进制文件格式(包含不可见字符，有独特的文件结构)、文本文件格式(全是可见字符)与数据库格式(存储在数据库文件中)。其中文本文件格式一般又分3种类型，包括键值对格式、json格式与XML格式。

[0053] 具体地，本发明实施例针对对象为需要使用文本格式的目标配置文件的软件或服务，首先，获取文本文件格式的目标配置文件。

[0054] S102：识别所述目标配置文件的文本文件格式类型，并确定所述目标配置文件的键值key-value对。

[0055] 具体地，识别目标配置文件采用的文本文件格式类型是键值对、json或是XML。

[0056] 对于键值对格式类型，一般文件中每行左边是一个标识符作为key，中间使用“=”连接，右边则是key对应的value。

[0057] 对于json格式而言，一般以“{”与“}”包裹主体，key与value用引号包裹并用“:”隔开。

[0058] 对于XML格式而言，主体为XML标签，并且key作为标签名而value作为标签值，或者key和value直接作为标签属性用“=”分隔。

[0059] 针对键值对、json或是XML的文本文件格式类型，确定所述目标配置文件的键值key-value对，定位key和value的位置。

[0060] S103：对以所述目标配置文件作为输入的程序进行预模糊测试以检测所述程序是否有格式上的漏洞，并提取所述程序中的所有可见字符串。

[0061] 其中，所述预模糊测试是使用模糊测试工具AFL对程序进行初步的模糊测试，以挖掘在目标配置文件格式错误的情况下的漏洞。

[0062] 具体地，首先，使用模糊测试工具AFL对以所述目标配置文件作为输入的程序进行预模糊测试，检测所述程序是否有格式上的漏洞，然后，从程序的.data段中通过遍历识别所有的可见字符串，每个可见字符串是以“\0”、“\r”、“\n”和“\t”作为结尾，在一个实施例中，为了便于后续步骤处理，识别所有的可见字符串后，将所有的可见字符串结尾字符统一换为“\0”。

[0063] 步骤S101-S103为对文本文件格式的目标配置文件的预处理。

[0064] S104：利用所述可见字符串，对所述目标配置文件的key-value对中的key进行变异，得到key组合种子文件。

[0065] 具体地，使用对文本文件格式的目标配置文件预处理中提取的可见字符串替换目标配置文件中的key，或直接在目标配置文件中增加新的key-value对，也能够直接删除目标配置文件中的key，再进行插桩执行判断，得到key组合种子文件。

[0066] 所述插桩执行是在被测程序中插入探针，然后通过探针的执行来获得程序的控制流和数据流信息，以此来实现测试的目的。需要说明的是，本发明实施例不对key本身进行

字节变异，因为如果仅仅key字节自身变异就存在漏洞一般能在预模糊测试中发现，而后续测试中如果key是错误的话往往会导致目标配置文件解析失败，增加很多无用的种子文件，大大降低测试效率。

[0067] S105：基于所述key组合种子文件中key的权重，对所述key组合种子文件中的key对应的value进行变异，得到新的组合种子文件。

[0068] 具体地，得到了步骤S104中确定的key组合种子文件，然后根据所述key组合种子文件中key的权重，对该key组合种子文件中的key对应的value进行变异，进行插桩执行判断，得到新的组合种子文件。需要说明的是，key将决定解析时执行的函数，而value往往是作为函数的执行参数。

[0069] S106：利用所述新的组合种子文件挖掘所述程序的漏洞。

[0070] 将步骤S105得到的所述新的组合种子文件作为输入的程序进行模糊测试，挖掘程序中较深层次的漏洞。

[0071] 本发明实施例提供了面向文本配置文件的模糊测试方法，该方法中，通过对以文本文件格式的目标配置文件作为输入的程序进行预模糊测试、key变异和value变异，得到新的组合种子文件后进行模糊测试，能够全面地挖掘程序中较深层次的漏洞，提升面向文本配置文件的模糊测试效率。

[0072] 进一步地，在上述发明实施例的基础上，所述利用所述可见字符串，对所述目标配置文件的key-value对中的key进行变异，得到key组合种子文件，具体包括：

[0073] 针对每个所述可见字符串，利用当前可见字符串替换所述key-value对中的key，得到种子文件，将所述种子文件作为输入插桩执行，若产生了新的执行路径，则将所述key存储至有效key集合；

[0074] 基于所述有效key集合，依次对所述种子文件中的key随机地进行删除、替换和增加操作中的任一种，得到key组合种子文件。

[0075] 具体地，首先，逐个使用预处理中提取的可见字符串替换目标配置文件中的key-value对中的key，在每替换一个key之后，就得到种子文件，将种子作为输入的程序插桩执行，若产生了新的执行路径，那么替换的可见字符串很可能是有效key，则将所述key存储至有效key集合，再提取最终的有效key集合。

[0076] 然后，依次对所述种子文件中的key随机地进行删除、替换和增加操作中的任一种，最终，得到key组合种子文件。对于替换key操作，是直接将预处理中定位的key位置替换为新的key即可。

[0077] 当目标配置文件采用的文本文件格式类型是键值对时，增加或删除key-value对操作，是直接匹配格式为“key＝value”的对应key-value行进行增加或删除即可。

[0078] 当目标配置文件采用的文本文件格式类型是json时，增加和删除key-value对操作，是直接匹配格式为‘“key”:“value”’的对应key-value项进行增加或删除即可。

[0079] 当目标配置文件采用的文本文件格式类型是XML时，增加或删除key-value对操作，需要先识别该key-value对所在的标签，直接增删整个标签即可；如果key-value是作为标签的属性存放在标签中，且标签还有其他属性，则仅增删标签属性而不增删标签；如果标签没有其他属性，则增删整个标签。

[0080] 本发明实施例提供了面向文本配置文件的模糊测试方法，该方法中，通过基于所

述有效key集合，依次对所述种子文件中的key随机地进行删除、替换和增加操作中的任一种，对key进行变异，得到key组合种子文件，能够更为全面地挖掘程序中的漏洞，提升面向文本配置文件的模糊测试效率。

[0081] 进一步地，在上述发明实施例的基础上，所述基于所述key组合种子文件中key的权重，对所述key组合种子文件中的key对应的value进行变异，得到新的组合种子文件，具体包括：

[0082] 针对所述key组合种子文件中的每个key对应的value进行变异，若判断插桩执行后产生了新的执行路径，根据所述新的执行路径中产生的新代码块数量设置对应key的权重；

[0083] 从权重高的前N个key中随机选取M个key，对所述M个key对应的value进行变异，若判断插桩执行后产生了新的执行路径，则同时增大所述M个key的权重，或者，若判断插桩执行后没有产生新的执行路径，则同时减小所述M个key的权重，若所述M个key中存在P个key的权重低于权重高的前N个key的权重，则重新从权重高的前N个key中随机选取M个key，直至所述M个key的权重都不大于权重阈值，得到新的组合种子文件；

[0084] 其中，N,M和P均为大于等于1的自然数，N≥M≥P。

[0085] 具体地，得到key组合种子文件后，首先，根据所述key组合种子文件中key的权重，逐个对该key组合种子文件中的key对应的value进行变异，若判断该变异后的种子文件进行插桩执行时产生了新的执行路径，则根据所述新的执行路径中产生的新代码块数量设置对应key的权重。例如，原本3个key的value分别是[1,2,3]，先对第一个key的value变异得到[xxxx,2,3]，然后保持第一个key原本的value，对第2个key的value变异得到[1,xxxxx,3]，最后对第3个key的value变异得到[1,2,xxxxxxx]，根据新出现的执行路径里的新代码块数量设置对应key的权重，新增代码块也是以初始value[1,2,3]时的路径作为对比，每增加一个新代码块对应key权重+1。需要说明的是，为了以示区别，用xxxx表示第一个key的value变异后的值，用xxxxx表示第2个key的value变异后的值，用xxxxxxx表示第3个key的value变异后的值，xxxx、xxxxx和xxxxxxx之间无关联。

[0086] 然后，从权重高的前N个key中随机选取M个key，对所述M个key对应的value进行变异，若判断该变异后的种子文件进行插桩执行时产生了新的执行路径，则同时增大所述M个key的权重，或者是，若判断该变异后的种子文件进行插桩执行时没有产生新的执行路径，则同时减小所述M个key的权重，若所述M个key中存在P个key的权重低于权重高的前N个key的权重，则重新从权重高的前N个key中随机选取M个key，直至所述M个key的权重都不大于权重阈值，得到新的组合种子文件。例如，设置好对应key的权重后，随机从权重高的10个key里选5个key，同时对他们的value进行变异。当出现新路径时，5个key的权重全部增加新增代码块数量；当没有新路径出现时，这5个key权重全部减1(这里的新路径是把以往的所有路径作为基础，目的更倾向于探索之前未走过的路径)。当选取的5个key中有2个key的权重低于前10时，则重新从前10个key中选5个key变异，重复以上过程。当所有key权重都变成1，这个key组合的value变异结束，得到新的组合种子文件。当多次value变异后仍未出现新的执行路径，则重新选取key组合种子文件。

[0087] 本发明实施例提供了面向文本配置文件的模糊测试方法，该方法中，通过根据所述新的执行路径中产生的新代码块数量设置对应key的权重，并从权重高的前N个key中随

机选取M个key，根据新的执行路径，调整M个key的权重，使得都不大于权重阈值，对value进行变异，得到新的组合种子文件，能够挖掘程序中较深层次的漏洞，提升面向文本配置文件的模糊测试效率。

[0088] 进一步地，在上述发明实施例的基础上，所述对所述key组合种子文件中的key对应的value进行变异，具体包括：

[0089] 循环执行以下步骤预设次数：随机选择一条操作策略对所述key组合种子文件中的Q个key对应的value进行变异；

[0090] 其中，所述预设次数根据所述key对应的value的数据长度确定；所述操作策略包括按位翻转，整数加减，数据插入和数据删减；Q为大于等于1的自然数。

[0091] 具体地，对所述key组合种子文件中的key对应的value进行变异，详细为循环执行以下步骤预设次数：随机选择一条操作策略对所述key组合种子文件中的Q个key对应的value进行变异；所述操作策略包括按位翻转，整数加减，数据插入和数据删减。例如，变异时将随机翻转value的某些bit、对随机的字节加减随机的整数、对随机的字按随机大端序、小端序加减随机整数、对随机的双字按随机大端序、小端序加减随机整数、对随机的字按随机大端序、小端序加减随机整数、选择随机的位置插入随机长度数据，其80％内容来自value自身，20％内容随机生成和选择随机的位置删除随机长度数据。循环从以上7个策略中随机选择一条策略进行变异，循环的预设次数设置为value的数据长度*(1到2之间的一个随机数)。

[0092] 本发明实施例提供了面向文本配置文件的模糊测试方法，该方法中，通过随机选择一条操作策略对所述key组合种子文件中的多个key对应的value进行变异，并循环执行预设次数，能够挖掘程序中较深层次的漏洞，提升面向文本配置文件的模糊测试效率。

[0093] 图3为本发明实施例提供的面向文本配置文件的模糊测试装置的结构示意图，如图3所示，所述装置包括：

[0094] 获取模块301，用于获取文本文件格式的目标配置文件；

[0095] 识别模块302，用于识别所述目标配置文件的文本文件格式类型，并确定所述目标配置文件的键值key-value对；

[0096] 检测提取模块303，用于对以所述目标配置文件作为输入的程序进行预模糊测试以检测所述程序是否有格式上的漏洞，并提取所述程序中的所有可见字符串；

[0097] key变异模块304，用于利用所述可见字符串，对所述目标配置文件的key-value对中的key进行变异，得到key组合种子文件；

[0098] value变异模块305，用于基于所述key组合种子文件中key的权重，对所述key组合种子文件中的key对应的value进行变异，得到新的组合种子文件；

[0099] 挖掘模块306，用于利用所述新的组合种子文件挖掘所述程序的漏洞。

[0100] 该面向文本配置文件的模糊测试装置用于实现前述各方法实施例提供的面向文本配置文件的模糊测试方法。因此，在前述各方法实施例中的描述和定义，可以用于本发明实施例提供的面向文本配置文件的模糊测试装置中各个执行模块的理解，在此不再赘述。

[0101] 本发明实施例提供了面向文本配置文件的模糊测试装置，该装置中，通过对以文本文件格式的目标配置文件作为输入的程序进行预模糊测试、key变异和value变异，得到新的组合种子文件，并进行模糊测试，能够全面地挖掘程序中较深层次的漏洞，提升面向文

本配置文件的模糊测试效率。

[0102] 进一步地,在上述发明实施例的基础上,所述key变异模块,具体用于:

[0103] 针对每个所述可见字符串,利用当前可见字符串替换所述key-value对中的key,得到种子文件,将所述种子文件作为输入插桩执行,若产生了新的执行路径,则将所述key存储至有效key集合;

[0104] 基于所述有效key集合,依次对所述种子文件中的key随机地进行删除、替换和增加操作中的任一种,得到key组合种子文件。

[0105] 进一步地,在上述发明实施例的基础上,所述value变异模块,具体用于:

[0106] 针对所述key组合种子文件中的每个key对应的value进行变异,若判断插桩执行后产生了新的执行路径,根据所述新的执行路径中产生的新代码块数量设置对应key的权重;

[0107] 从权重高的前N个key中随机选取M个key,对所述M个key对应的value进行变异,若判断插桩执行后产生了新的执行路径,则同时增大所述M个key的权重,或者,若判断插桩执行后没有产生新的执行路径,则同时减小所述M个key的权重,若所述M个key中存在P个key的权重低于权重高的前N个key的权重,则重新从权重高的前N个key中随机选取M个key,直至所述M个key的权重都不大于权重阈值,得到新的组合种子文件;

[0108] 其中,N,M和P均为大于等于1的自然数,N≥M≥P。

[0109] 进一步地,所述value变异模块,具体还用于:

[0110] 循环执行以下步骤预设次数:随机选择一条操作策略对所述key组合种子文件中的Q个key对应的value进行变异;

[0111] 其中,所述预设次数根据所述key对应的value的数据长度确定;所述操作策略包括按位翻转,整数加减,数据插入和数据删减;Q为大于等于1的自然数。

[0112] 图4示例了一种电子设备的实体结构示意图,如图4所示,该电子设备可以包括:处理器(Processor)401、存储器(Memory)402、通信接口(Communications Interface)403和通信总线404,其中,处理器401,存储器402,通信接口403通过通信总线404完成相互间的通信。处理器401可以调用存储器402中的逻辑指令,以执行上述各方法实施例所提供的方法,例如包括:获取文本文件格式的目标配置文件;识别所述目标配置文件的文本文件格式类型,并确定所述目标配置文件的键值key-value对;对以所述目标配置文件作为输入的程序进行预模糊测试以检测所述程序是否有格式上的漏洞,并提取所述程序中的所有可见字符串;利用所述可见字符串,对所述目标配置文件的key-value对中的key进行变异,得到key组合种子文件;基于所述key组合种子文件中key的权重,对所述key组合种子文件中的key对应的value进行变异,得到新的组合种子文件;利用所述新的组合种子文件挖掘所述程序的漏洞。

[0113] 此外,上述的存储器402中的逻辑指令可以通过软件功能单元的形式实现并作为独立的产品销售或使用时,可以存储在一个计算机可读取存储介质中。基于这样的理解,本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括:U盘、移动硬盘、只读存储器(ROM,

Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0114] 本发明实施例还提供非暂态计算机可读存储介质,其上存储有计算机程序,该计算机程序被处理器执行时实现以执行上述各方法实施例所提供的方法,例如包括:获取文本文件格式的目标配置文件;识别所述目标配置文件的文本文件格式类型,并确定所述目标配置文件的键值key-value对;对以所述目标配置文件作为输入的程序进行预模糊测试以检测所述程序是否有格式上的漏洞,并提取所述程序中的所有可见字符串;利用所述可见字符串,对所述目标配置文件的key-value对中的key进行变异,得到key组合种子文件;基于所述key组合种子文件中key的权重,对所述key组合种子文件中的key对应的value进行变异,得到新的组合种子文件;利用所述新的组合种子文件挖掘所述程序的漏洞。

[0115] 以上所描述的装置实施例仅仅是示意性的,其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性的劳动的情况下,即可以理解并实施。

[0116] 通过以上的实施方式的描述,本领域的技术人员可以清楚地了解到各实施方式可借助软件加必需的通用硬件平台的方式来实现,当然也可以通过硬件。基于这样的理解,上述技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品可以存储在计算机可读存储介质中,如ROM/RAM、磁碟、光盘等,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)执行各个实施例或者实施例的某些部分所述的方法。

[0117] 最后应说明的是:以上实施例仅用以说明本发明的技术方案,而非对其限制;尽管参照前述实施例对本发明进行了详细的说明,本领域的普通技术人员应当理解:其依然可以对前述各实施例所记载的技术方案进行修改,或者对其中部分技术特征进行等同替换;而这些修改或者替换,并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

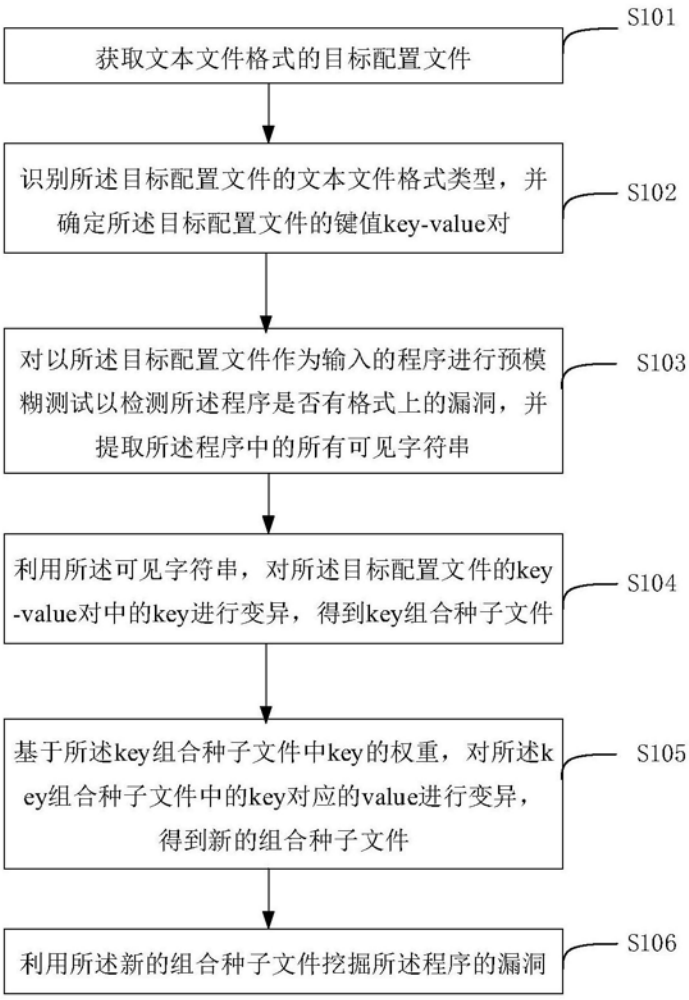

S101
获取文本文件格式的目标配置文件
识别所述目标配置文件的文本文件格式类型，并确定所述目标配置文件的键值key-value对
S102
对以所述目标配置文件作为输入的程序进行预模糊测试以检测所述程序是否有格式上的漏洞，并提取所述程序中的所有可见字符串
S103
利用所述可见字符串，对所述目标配置文件的key-value对中的key进行变异，得到key组合种子文件
S104
基于所述key组合种子文件中key的权重，对所述key组合种子文件中的key对应的value进行变异，得到新的组合种子文件
S105
利用所述新的组合种子文件挖掘所述程序的漏洞
S106

图1

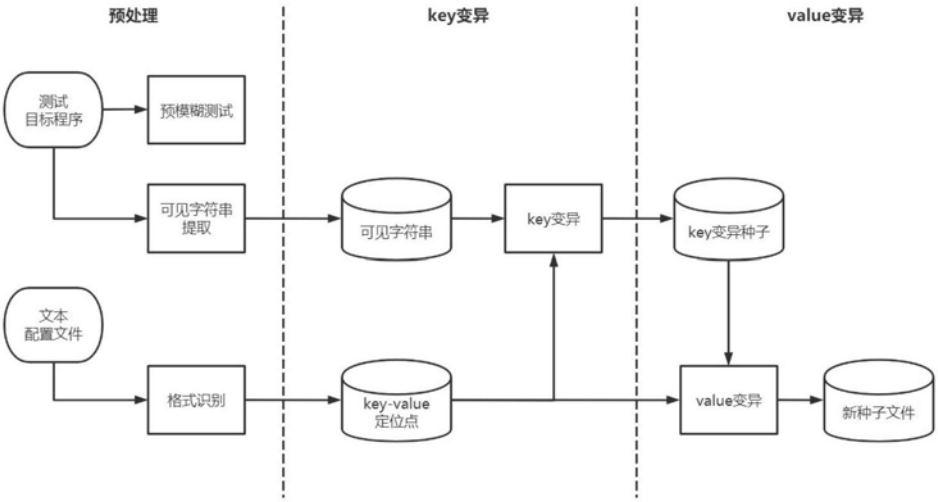

预处理
key变异
value变异
测试目标程序
预模糊测试
可见字符串提取
可见字符串
key变异
key变异种子
文本配置文件
格式识别
key-value定位点
value变异
新种子文件

图2

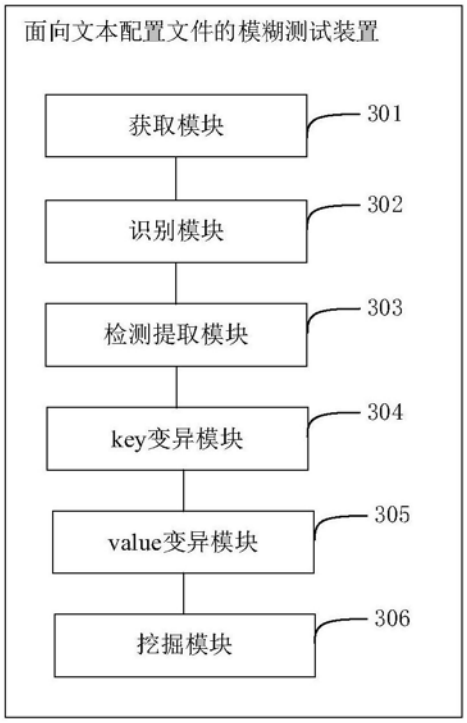

面向文本配置文件的模糊测试装置
获取模块
301
识别模块
302
检测提取模块
303
key变异模块
304
value变异模块
305
挖掘模块
306

图3

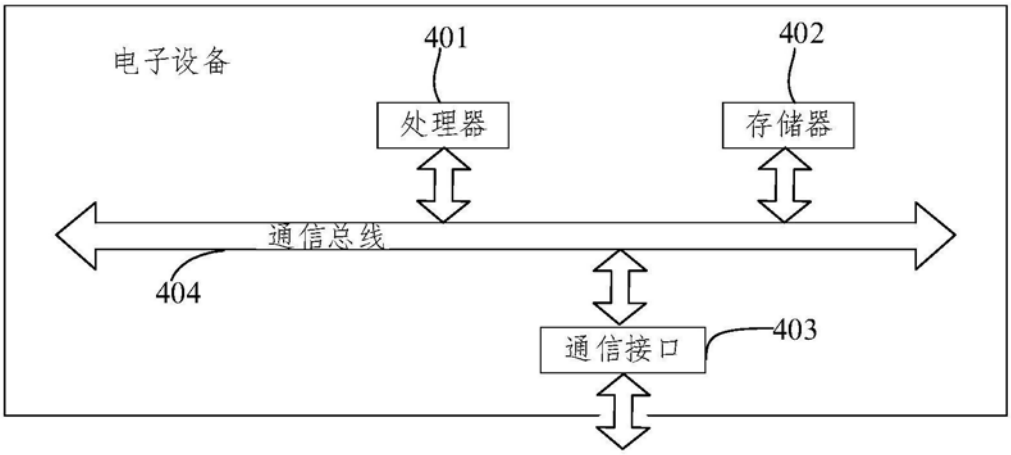

电子设备
401
处理器
402
存储器
通信总线
404
通信接口
403

图4