(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 118331649 A
(43)申请公布日 2024.07.12

(21)申请号 202410032499.8

(22)申请日 2024.01.09

(30)优先权数据
102023200113.6 2023.01.10 DE

(71)申请人 罗伯特·博世有限公司
地址 德国斯图加特

(72)发明人 P·杜普利斯

(74)专利代理机构 中国专利代理(香港)有限公司 72001
专利代理师 臧永杰 刘春元

(51)Int.Cl.
G06F 9/445(2018.01)
G06F 16/242(2019.01)
G06F 16/2453(2019.01)

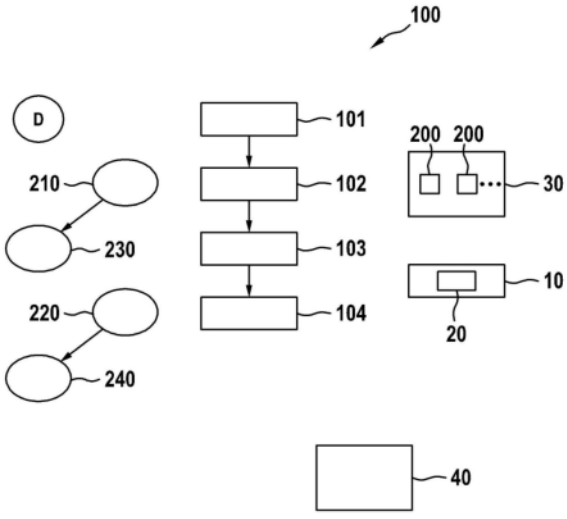
权利要求书2页 说明书7页 附图3页

(54)发明名称

用于确定产品的安全相关薄弱环节的相关性的方法

(57)摘要

本发明涉及用于确定产品(30)的安全相关薄弱环节的相关性的方法(100),所述方法包括自动化地被执行的以下步骤:-提供(101)术语规范(D),所述术语规范包括用于详细说明薄弱环节的术语,-提供(102)所述产品(30)的产品配置文件(230),所述产品配置文件基于所述术语规范(D)的术语详细说明所述产品(30),-针对相应薄弱环节提供(103)至少一个薄弱环节配置文件(240),所述薄弱环节配置文件基于所述术语规范(D)的术语详细说明所述薄弱环节,-基于所述产品配置文件(230)和所述薄弱环节配置文件(240)的处理来确定(104)所述相应薄弱环节与所述产品(30)的相关性。



CN 118331649 A

1.一种用于确定产品(30)的安全相关薄弱环节的相关性的方法(100),所述方法包括自动化地被执行的以下步骤:

-提供(101)术语规范(D),所述术语规范包括用于详细说明薄弱环节的术语,

-提供(102)所述产品(30)的产品配置文件(230),所述产品配置文件基于所述术语规范(D)的术语详细说明所述产品(30),

-针对相应薄弱环节提供(103)至少一个薄弱环节配置文件(240),所述薄弱环节配置文件基于所述术语规范(D)的术语详细说明所述薄弱环节,

-基于所述产品配置文件(230)和所述薄弱环节配置文件(240)的处理来确定(104)所述相应薄弱环节与所述产品(30)的相关性。

2.根据权利要求1所述的方法(100),其特征在于,

提供(101)所述术语规范(D)包括以下步骤:

-从至少一个薄弱环节规范(220)、优选地关于已知薄弱环节的公共数据库中确定所述相应薄弱环节的薄弱环节描述,其中优选地所述薄弱环节描述按照所述薄弱环节详细说明至少一种攻击可能性,其中优选地所述至少一种攻击可能性说明至少一个条件,在所述条件下利用所述薄弱环节是可能的,

-优选地通过语言处理、优选地自然语言处理技术,基于所述薄弱环节描述来确定所述术语规范(D)的术语,其中特别优选地从所述薄弱环节描述中提取所述术语。

3.根据前述权利要求中任一项所述的方法(100),其特征在于,

提供(102)所述产品配置文件(230)包括以下步骤:

-定义产品嵌入(P),其中为此所述术语规范(D)的术语鉴于其与所述产品(30)的相关性被标记,以便通过所标记的术语来描述所述产品(30),优选地通过将所述术语与产品规范(210)进行对比来进行,其中所述产品规范(210)鉴于所述产品(30)的至少一个软件组件(200)详细说明所述产品(30)。

4.根据前述权利要求中任一项所述的方法(100),其特征在于,

提供(103)所述薄弱环节配置文件(240)包括以下步骤:

-从薄弱环节规范(220)、优选地公共数据库中确定当前安全相关薄弱环节的薄弱环节描述,其中所述薄弱环节描述优选地按照所述当前薄弱环节详细说明至少一种攻击可能性,其中优选地所述至少一种攻击可能性说明至少一个条件,在所述条件下利用所述当前薄弱环节是可能的,

-定义薄弱环节嵌入(V),其中为此所述术语规范(D)的术语鉴于其与所述当前薄弱环节的相关性被标记,以便通过所标记的术语描述所述当前薄弱环节,优选地通过将所述术语与所确定的薄弱环节描述进行对比来进行。

5.根据前述权利要求中任一项所述的方法(100),其特征在于,

确定(104)所述相关性包括以下步骤:

-优选地通过计算距离、特别优选地汉明距离和/或基于语言处理形式的处理,确定所述产品配置文件(230)、优选地所述产品嵌入(P)与针对所述相应薄弱环节的薄弱环节配置文件(240)、优选地所述薄弱环节嵌入(V)的相似性,

-基于所确定的相似性定义所述相应薄弱环节的相关性。

6.根据前述权利要求中任一项所述的方法(100),其特征在于,

提供(102)所述产品配置文件(230)包括以下步骤：

-基于所述术语规范(D)的术语定义查询术语，其中所述查询术语详细说明所述产品(30)

其中提供(103)所述薄弱环节配置文件(240)包括针对所述相应薄弱环节执行的以下步骤：

-基于所定义的查询术语确定所述相应薄弱环节的薄弱环节描述的基于查询的摘要，优选地以便按照所述查询术语过滤所述薄弱环节描述，

其中确定(104)所述相关性包括以下步骤：

-基于所确定的基于查询的摘要、优选地基于在所述薄弱环节描述中出现的查询术语的数量来定义所述相关性。

7.根据前述权利要求中任一项所述的方法(100)，其特征在于，

针对多个薄弱环节提供(103)所述薄弱环节配置文件并且确定(104)所述相关性，其中所述薄弱环节根据其分别确定的相关性被输出。

8.根据前述权利要求中任一项所述的方法(100)，其特征在于，

所述产品(30)被设置用于控制机器(40)、优选地车辆(40)和/或机器人(40)，其中所述方法(100)的步骤自动地重复地被执行，优选地通过云服务被执行，尤其是用于在运行所述机器(40)期间监控所述产品(30)的信息安全性。

9.一种计算机程序(20)，所述计算机程序包括指令，当通过计算机(10)执行所述计算机程序(20)时，所述指令促使所述计算机(10)执行根据前述权利要求中任一项所述的方法(100)。

10.一种用于进行数据处理的设备(10)，所述设备被设立用于执行根据权利要求1至8中任一项所述的方法(100)。

用于确定产品的安全相关薄弱环节的相关性的方法

技术领域

[0001] 本发明涉及一种用于确定产品的安全相关薄弱环节的相关性的方法。本发明此外涉及用于此目的的计算机程序以及设备。

背景技术

[0002] 已知的是,安全相关产品在其开发阶段中鉴于已知的薄弱环节被检验。这经常通过将所谓的“漏洞数据库(Vulnerability database)”、即薄弱环节数据库、诸如NVD(国家漏洞数据库(National Vulnerability Database))或类似数据库与软件物料清单(Software Bill ofMaterials,SBOM)进行对比来发生,在所述软件物料清单中举出了在相应的产品中使用的软件组件。从安全角度来看,这种鉴于已知薄弱环节的检验是非常值得期望的,并且常常得出在薄弱环节数据库中包含的已知薄弱环节的长列表。然而,在此经常不清楚这些所报告的薄弱环节中的哪些薄弱环节实际上与特定产品是相关的。例如,在NVD中列出针对Linux内核4.14的大约6000个已知的安全漏洞。然而,仅当对应的内核函数实际上被使用并且当差错(Fehler)——鉴于产品的规范及其软件配置——在实践中实际上可以被利用时,这些差错中的每一个差错才是与特定的产品相关的。

发明内容

[0003] 本发明的主题是具有权利要求1的特征的方法、具有权利要求9的特征的计算机程序以及具有权利要求10的特征的设备。本发明的其他特征和细节从相应的从属权利要求、说明书和附图中得出。在此,结合根据本发明的方法描述的特征和细节当然也结合根据本发明的计算机程序以及根据本发明的设备适用,并且分别反之亦然,使得关于针对各个发明方面的公开始终被相互参考或者可以被相互参考。

[0004] 尤其是,本发明的主题是一种用于确定产品、优选地软件产品的安全相关薄弱环节(英语:vulnerabilities(漏洞))、优选地软件薄弱环节的相关性的方法,优选地以便以这种方式执行产品的自动检验。该产品可以具有软件和/或硬件组件。薄弱环节(Schwachstellen)可以是软件组件、但是必要时也为硬件组件的信息技术薄弱环节。在此情况下,该方法可以包括以下步骤,所述步骤可以至少部分地重复地和/或依次和/或自动化地被执行:

[0005] -提供术语规范、优选地数字词典,所述术语规范包括用于详细说明薄弱环节(并且尤其是也通常与具体产品无关地详细说明安全相关薄弱环节)的术语,

[0006] -提供产品的产品配置文件,所述产品配置文件基于所述术语规范的术语优选地在使用术语规范的术语的情况下、优选地基于SBOM等详细说明产品,

[0007] -针对相应薄弱环节、优选地针对薄弱环节中的每个薄弱环节提供至少一个薄弱环节配置文件,其中优选地在使用术语规范的术语的情况下并且优选地在使用也已经被使用来提供产品配置文件的相同术语的情况下,相应的薄弱环节配置文件基于术语规范的术语详细说明相应薄弱环节,

[0008] -基于(针对相应薄弱环节的)产品配置文件和薄弱环节配置文件的处理来确定相应薄弱环节、优选地薄弱环节中的每个薄弱环节与所述产品的相关性。

[0009] 因此,本发明具有以下优点:能够自动化地并且可靠地针对特定产品确定相关薄弱环节。大多数软件薄弱环节只能在特定的条件下被利用。因此即使在特定产品中使用软件组件的易受攻击的(英语:vulnerable)版本,也不清楚该薄弱环节是否实际上可以被利用。这常常与以下相关联,即标准SBOM不包含关于在产品的情况下是否存在这些特定条件的信息(这些条件的存在在下面尤其是也被称为攻击可能性)。因此,根据具有已知薄弱环节的数据库检验产品导致大数量的误警报,必须手动地消除所述误警报。随之出现用于这样的产品的差错检验的高耗费。因此,本发明的优点可以是,在尤其是针对已知薄弱环节数据库的基于SBOM的产品检验的情况下,可以根据所确定的相关性自动地排除假阳性结果或者至少可以减少其数量。

[0010] 可以例如基于针对具体产品的薄弱环节报告和SBOM以及必要时针对具体产品的源代码提供产品配置文件和/或相应的薄弱环节配置文件。然后可以自动地确定来自诸如NVD之类的数据库中的已知薄弱环节中的哪些薄弱环节实际上是与该产品相关的。尤其是当库的特定易受攻击函数或Linux内核的特定易受攻击特征实际上被使用在该产品的源代码中时,与该产品的相关性存在。

[0011] 有利地,在本发明的情况下可以规定,提供术语规范包括以下步骤:

[0012] -从至少一个薄弱环节规范、优选地诸如NVD之类的关于已知薄弱环节的公共数据库中确定相应薄弱环节的薄弱环节描述、优选地文本薄弱环节描述,其中优选地所述薄弱环节描述按照薄弱环节详细说明至少一种攻击可能性,其中优选地所述至少一种攻击可能性说明至少一个条件,在所述条件下利用薄弱环节是可能的,

[0013] -优选地通过语言处理、优选地自然语言处理技术,基于薄弱环节描述来确定术语规范的术语,其中特别优选地从薄弱环节描述中提取术语。

[0014] 这使得能够可以将术语规范构建为具有在薄弱环节规范中用于描述薄弱环节所使用的这样的术语的词典。在此,至少一个薄弱环节规范例如包括可公开访问的数据库,其中鉴于攻击可能性描述薄弱环节。例如,在薄弱环节描述中鉴于为了利用薄弱环节而必须存在的技术条件和/或软件组件来在语言上描述薄弱环节。在此,薄弱环节描述可以包括通过自然语言、尤其是在NLP(Natural Language Processing(自然语言处理))的意义上的描述。为此,薄弱环节描述可以使用术语规范的术语。

[0015] 如果在本发明的范围内提供产品配置文件包括以下步骤:

[0016] -定义产品嵌入,其中为此术语规范的术语鉴于其与产品的相关性被标记,以便通过所标记的术语来描述产品,优选地通过将术语与产品规范、优选地文本产品规范进行对比来进行,其中产品规范鉴于产品的至少一个软件组件详细说明产品,则可能是有利的。

[0017] 如果术语出现在产品规范中,则这些术语可以例如被标记为与产品相关的。否则,这些术语可以必要时被标记为不相关的。于是,产品嵌入可以包括这些标记。可能的是,产品规范在使用术语规范的术语的情况下描述产品。产品规范可以例如包括产品的软件组件的命名和/或关于软件组件的其他技术详情。在此可能的是,产品规范通过自然语言、尤其是在NLP意义上描述产品。这具有以下优点,即必要时已经存在并且被设置用于通过人类解释的产品的描述可以被使用来自动地检验产品。

[0018] 此外可设想的是,提供薄弱环节配置文件包括以下步骤:

[0019] -从薄弱环节规范、优选地诸如NVD之类的公共数据库中确定所述安全相关薄弱环节以及优选地当前安全相关薄弱环节的薄弱环节描述、优选地文本薄弱环节描述,其中薄弱环节描述优选地按照当前薄弱环节详细说明至少一种攻击可能性,其中优选地所述至少一种攻击可能性说明至少一个条件,在所述条件下利用所述当前薄弱环节是可能的,

[0020] -定义薄弱环节嵌入,其中为此术语规范的术语鉴于其与当前薄弱环节的相关性被标记,以便通过所标记的术语描述当前薄弱环节,优选地通过将术语与所确定的薄弱环节描述进行对比来进行。

[0021] 如果术语出现在薄弱环节规范中,则这些术语可以例如被标记为与薄弱环节相关的。否则,这些术语可以必要时被标记为不相关的。于是,薄弱环节嵌入可以包括这些标记。可能的是,薄弱环节规范在使用术语规范的术语的情况下描述薄弱环节。薄弱环节规范可以例如包括软件组件的命名和/或关于软件组件的其他技术详情。在此可能的是,薄弱环节规范通过自然语言、尤其是在NLP意义上描述薄弱环节。这具有以下优点,即必要时已经存在并且被设置用于通过人类解释的薄弱环节的描述可以被使用来自动地检验产品或确定相关性。在此,当前薄弱环节可以是当前、即在检验或确定相关性的时间点从薄弱环节规范中检索的薄弱环节。这可能与以下相关联,即薄弱环节规范重复地被更新,以便描述新的薄弱环节。

[0022] 此外,在本发明的范围内可能有利的是,确定相关性包括以下步骤,优选地针对薄弱环节中的每个薄弱环节执行这些步骤:

[0023] -优选地通过计算距离、特别优选地汉明距离,和/或基于语言处理形式的处理,确定产品配置文件、优选地产品嵌入与针对相应薄弱环节的薄弱环节配置文件、优选地薄弱环节嵌入的相似性,

[0024] -基于所确定的相似性定义相应薄弱环节的相关性。

[0025] 换句话说,为了确定相关性,可以比较产品配置文件和相应薄弱环节配置文件(在语言上)多么一致。以这种方式可以根据所属的薄弱环节配置文件对于薄弱环节中的每个薄弱环节确定该薄弱环节的相关性。

[0026] 根据另一优点可以规定,提供产品配置文件包括以下步骤:

[0027] -基于术语规范的术语定义查询术语,其中查询术语详细说明产品。

[0028] 查询术语可以被设置用于对相应薄弱环节的薄弱环节描述进行查询,以便基于查询术语获得摘要(Zusammenfassung)。例如,摘要可以特定于薄弱环节描述中的查询术语的频率。例如,查询术语可以根据在产品规范和/或产品嵌入中设置的术语被定义。

[0029] 此外,提供薄弱环节配置文件可以包括以下步骤,所述步骤针对相应薄弱环节被执行并且优选地针对薄弱环节中的每个薄弱环节被执行:基于所定义的查询术语确定相应薄弱环节的薄弱环节描述的基于查询的摘要,优选地以便按照查询术语过滤薄弱环节描述。

[0030] 在此,确定相关性可以包括以下步骤:基于所确定的基于查询的摘要、优选地基于在薄弱环节描述中出现的查询术语的数量和/或频率来定义相关性。这使得能够可靠地确定相关性。

[0031] 所确定的相关性可以例如指示:薄弱环节在具体产品的情况下是否可以被利用。

在此,相关性可以例如具有分类。此外,在本发明的范围内,可设想的是,针对多个薄弱环节提供薄弱环节配置文件并且确定相关性,其中薄弱环节根据其分别确定的相关性被输出。这使得能够对于产品可靠地评估安全性。

[0032] 此外,可设想的是,该产品被设置用于控制机器、优选地车辆、诸如机动车辆和/或自主车辆和/或机器人。在此,所述方法的步骤可以自动地重复地被执行,优选地通过云服务被执行,尤其是用于在运行机器期间监控产品的信息安全性。例如,车辆可以自动地被控制,例如通过自主驾驶功能和/或驾驶员辅助系统被控制,所述驾驶员辅助系统至少部分由产品提供。

[0033] 本发明的主题同样是一种计算机程序、尤其是计算机程序产品,其包括指令,当通过计算机执行计算机程序时,所述指令促使所述计算机执行根据本发明的方法。因此,根据本发明的计算机程序引起如参考根据本发明的方法已经详尽描述的相同的优点。

[0034] 本发明的主题同样是一种用于进行数据处理的设备,所述设备被设立用于执行根据本发明的方法。例如,可以设置执行根据本发明的计算机程序的计算机作为设备。计算机可以具有至少一个用于执行计算机程序的处理器。还可以设置非易失性数据存储器,在所述非易失性数据存储器中可以储存计算机程序并且通过处理器可以从所述非易失性数据存储器中读出计算机程序用于执行。

[0035] 本发明的主题同样可以是一种计算机可读存储介质,所述计算机可读存储介质包括根据本发明的计算机程序。存储介质例如被构造为数据存储器、诸如硬盘和/或非易失性存储器和/或存储卡。存储介质可以例如集成到计算机中。

[0036] 此外,根据本发明的方法还可以被实施为计算机实现的方法。

附图说明

[0037] 本发明的其他优点、特征和详情从以下描述中得出,其中参考附图详细地描述本发明的实施例。在此,在权利要求中和在说明书中提及的特征可以分别单独地或以任意组合的方式是发明重要的。其中:

[0038] 图1示出根据本发明的实施例的方法、设备和计算机程序的示意性可视化。

[0039] 图2示出本发明的另一实施变型方案的示意图。

[0040] 图3示出本发明的另一实施变型方案的示意图。

具体实施方式

[0041] 在下面的图中,对于也来自不同实施例的相同技术特征使用相同的附图标记。

[0042] 在图1中示出根据本发明的实施例的用于确定产品30的安全相关薄弱环节的相关性的方法100。根据第一方法步骤101,方法100包括提供术语规范(Begriffsspezifikation)D,所述术语规范包括用于详细说明薄弱环节的术语。换句话说,术语规范D可以被理解为词典,所述词典包括大量术语的汇编,所述术语可以被使用来描述薄弱环节以及必要时其攻击可能性。攻击可能性可以例如说明软件组件200的特定版本,所述特定版本在产品30的情况下必须被设置为条件,以便薄弱环节可能被攻击者利用并且可能引起损害。因此,攻击可能性必要时也可以被称为用于利用薄弱环节的条件。

[0043] 此外,根据第二方法步骤102,该方法100包括提供产品30的产品配置文件

(Produktprofil)230,所述产品配置文件可以基于术语规范D的术语来详细说明产品30。换句话说,产品配置文件230可以使用术语规范D的术语,以便描述产品30的软件组件200和/或在产品30的情况下具体存在的攻击可能性。这可以例如是软件组件200的清单。然而,有利地,产品配置文件230包括根据术语规范D的术语在产品规范210中的出现对所述术语的标记。产品规范210例如是以用于通过用户使用的文本形式以及必要时以自然语言的产品30的技术规范。

[0044] 此外,设置第三方法步骤103,其中为相应的薄弱环节提供薄弱环节配置文件240。在此,相应的薄弱环节配置文件240可以基于术语规范D的术语来详细说明相应的薄弱环节。在这里,也可设想的是,薄弱环节配置文件240包括根据术语规范D的术语在薄弱环节规范220中的出现对所述术语的标记。薄弱环节规范220可以以用于通过用户使用的文本形式以及必要时以自然语言的相应薄弱环节的技术规范。

[0045] 根据第四方法步骤104,基于产品配置文件230和薄弱环节配置文件240的处理优选地全自动地确定相应薄弱环节与产品30的相关性。

[0046] 此外,在图1中示出用于执行方法100的计算机程序20以及用于执行方法100的设备10。此外示出,产品30可以被设置用于控制机器40、优选地车辆40和/或机器人40。此外,示出产品30可以具有一个或多个软件组件200,所述软件组件分别可以提供用于利用相应薄弱环节的攻击可能性。在此,可以是方法100的应用目的的是鉴于通过软件组件200提供的攻击可能性评估已知薄弱环节的相关性。

[0047] 为了获得术语规范D,可以首先规定从至少一个薄弱环节规范220中确定相应薄弱环节的薄弱环节描述。薄弱环节描述可以包括可以在哪些条件下利用薄弱环节的技术描述。这些条件可以例如包括存在通过软件组件200的攻击可能性。

[0048] 本发明的实施例的其他详情在图2和3中示出。在此,尤其是基础想法是借助自然语言处理(英语:Natural Language Processing,简称NLP)对薄弱环节描述进行分析。在此情况下,可以使用NLP的所谓文本摘要。如在“Sarkar,D.(2019).Text Analytics with Python:aPractitioner’s Guide to Natural Language Processing(pp.1-674).Bangalore:Apress”中描述的,在由文本文档的语料库(所述语料库可以是文本、段落或句子的汇编)组成的文本摘要的情况下可以创建摘要,所述摘要包含文本文档或汇编的最重要的点。在此,所谓的基于查询的摘要提供基于特定文本查询的文本摘要。也就是说,提取与这些特定查询相关的查询术语,诸如关键词和短语。

[0049] 根据本发明的实施变型方案的另一基本思想在于,(基于查询的)文本摘要可以被应用于各个薄弱环节描述。随后可以使用这些经压缩的信息来估计特定薄弱环节与所涉及的产品30相关的概率。

[0050] 在根据图3的实施例中,在初始化步骤301之后,例如提供102产品配置文件230可以包括基于术语规范D的术语来定义这样的查询术语305,其中查询术语详细说明产品30。此外,对于薄弱环节中的每个薄弱环节提供103薄弱环节配置文件240可以包括基于所定义的查询术语305确定相应薄弱环节的薄弱环节描述的基于查询的摘要306,优选地以便根据查询术语305过滤薄弱环节描述。随后可以基于所确定的基于查询的摘要306、优选地基于出现在薄弱环节描述中的查询术语305的数量来定义相关性。然后可以输出303与产品30相关的薄弱环节的列表304。在此,薄弱环节可能根据例如按顺序分别确定的其相关性被输

出。

[0051] 根据在图2和3中所示的本发明的实施变型方案,可以设置用于初始化的第一步骤301。示出初始化步骤301可以重复地被执行,以便通过更新过程302重复地确定当前薄弱环节的薄弱环节描述。在该第一步骤301期间,可以从薄弱环节规范220、尤其是公共数据库、诸如NVD(英语:National Vulnerability Database(国家漏洞数据库))、GitHub安全公告或软件提供商的安全提示中检索大数量的已知薄弱环节。在该检索时确定薄弱环节描述,所述薄弱环节描述优选地以自然语言描述薄弱环节。随后,可以基于薄弱环节描述以具有特征性术语(关键词)的词典D的形式创建术语规范D,所述特征性术语被使用来以安全漏洞的形式描述薄弱环节。这可以以自动化的方式发生,例如在使用如诸如“词频-反文档频率(term frequency-inverse document frequency,TF-IDF)”的NLP技术之类的语言处理并且移除标准停止词(“和”、“这个”等)以及标准安全术语、诸如“攻击(英语:attack)”、“薄弱环节”或“漏洞(英语:vulnerability)”等的情况下发生。可替代地或附加地,同样可能的是,这以半自动的方式发生,优选地通过专家发生,所述专家检验并且扩展具有用于描述在实践中可以利用薄弱环节的情况的术语和关键词的词典D。例如,专家可以利用来自操作系统的术语、诸如“网络”、“TCP”、“IP”、“根(Root)”等来扩展词典D(如果在自动术语提取之后这些术语尚未已经包含在D中的话)。

[0052] 可选地,可以要么基于特定的触发器(Auslöser)(例如数据库中的k个新的项)要么基于时间段(例如每隔3个月)给词典D扩展新接纳到数据库中的薄弱环节。这由更新过程302被可视化。

[0053] 在图2中所示的本发明的实施变型方案的情况下,可以在使用来自词典D的术语的情况下为特定产品30创建描述P(也称为嵌入P或英语:Embedding)。换句话说,可以定义产品嵌入P,其中为此术语规范D的术语鉴于其与产品30的相关性被标记,以便通过所标记的术语来描述产品30,优选地通过将术语与产品规范210进行对比来进行。在此,术语规范210可以鉴于产品30的至少一个软件组件200详细说明产品30和/或从非易失性存储器和/或数据库中被检索。产品描述P可以例如是大向量,所述大向量在产品描述中包含来自D的对应术语的每个点处都具有“1”。在下一步骤中,对于在诸如NVD之类的数据库中发现的每个薄弱环节(也称为英语:vulnerability(漏洞)),可以使用文本薄弱环节描述,以便根据词典D中的术语计算薄弱环节嵌入V(或英语:vulnerability Embedding(漏洞嵌入))。嵌入V可以根据D中的术语来描述薄弱环节。随后(对于在数据库中发现的每个薄弱环节)可以根据两个嵌入P和V计算P和V之间的间距l。例如,这可以通过计算这两个向量之间的汉明距离(或在机器学习时使用的其他距离度量)来进行。给要评估的薄弱环节分派值l。最后,可以创建薄弱环节的列表304,所述薄弱环节根据其间距l以升序排列。该列表可以被使用来设置应该首先检验哪些薄弱环节的优先级。其背后的思考是,其描述包含更多可以在产品描述中发现的关键词的薄弱环节以更大的概率是相关的。

[0054] 对于在图3中所示的本发明的实施变型方案,可以利用查询术语305、即描述特定产品30的关键词来定义一组查询。对于这些查询所使用的的关键词可以是在D词典中可以发现的术语。随后可以针对在诸如NVD之类的数据库中发现的每个薄弱环节执行薄弱环节描述的基于查询的摘要306。因此,可以基于特定查询来过滤描述。对于在数据库中发现的每个薄弱环节,该步骤的结果可以是与上面提到的查询相关的一系列关键词和表达S。最

后,可以创建从薄弱环节数据库中检索的薄弱环节的列表304,其中薄弱环节按照在对应的集合S中的关键词的数量排列(可选地,可以对关键词进行加权)。该列表304可以按升序排序并且可以被使用来设置应该首先检验哪些薄弱环节的优先级。所基于的考虑是,其描述在描述所涉及的产品的查询的结果中包含更多关键词的薄弱环节以更大的概率是相关的。

[0055] 本发明的实施例使得能够可以执行关于给定的薄弱环节是否实际上与特定产品30相关的合理性检验。在此,该检验可以以自动化的方式被执行,并且以基于概率的顺序集中于薄弱环节。

[0056] 实施方式的上述阐述仅仅在示例的范围中描述本发明。当然,只要在技术上有意义,实施方式的各个特征可以自由地被相互组合,而不脱离本发明的范围。

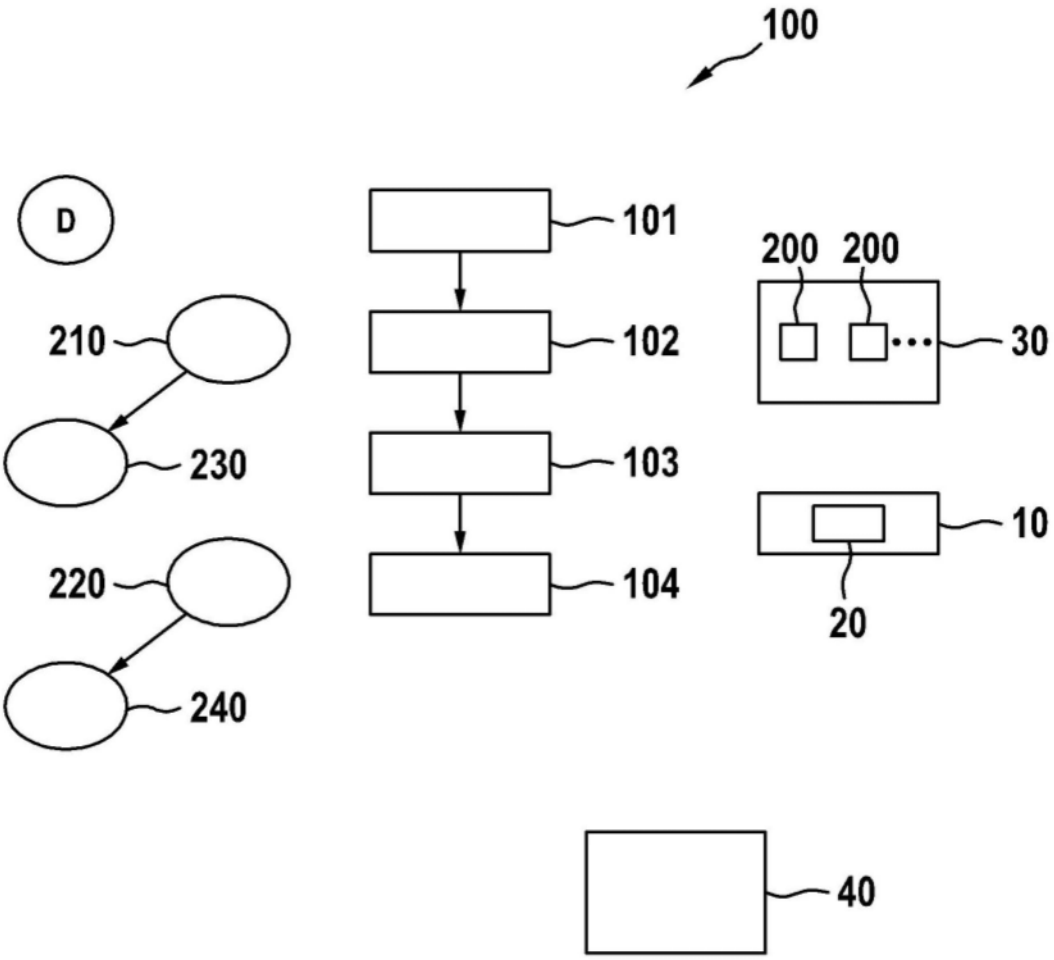


图1

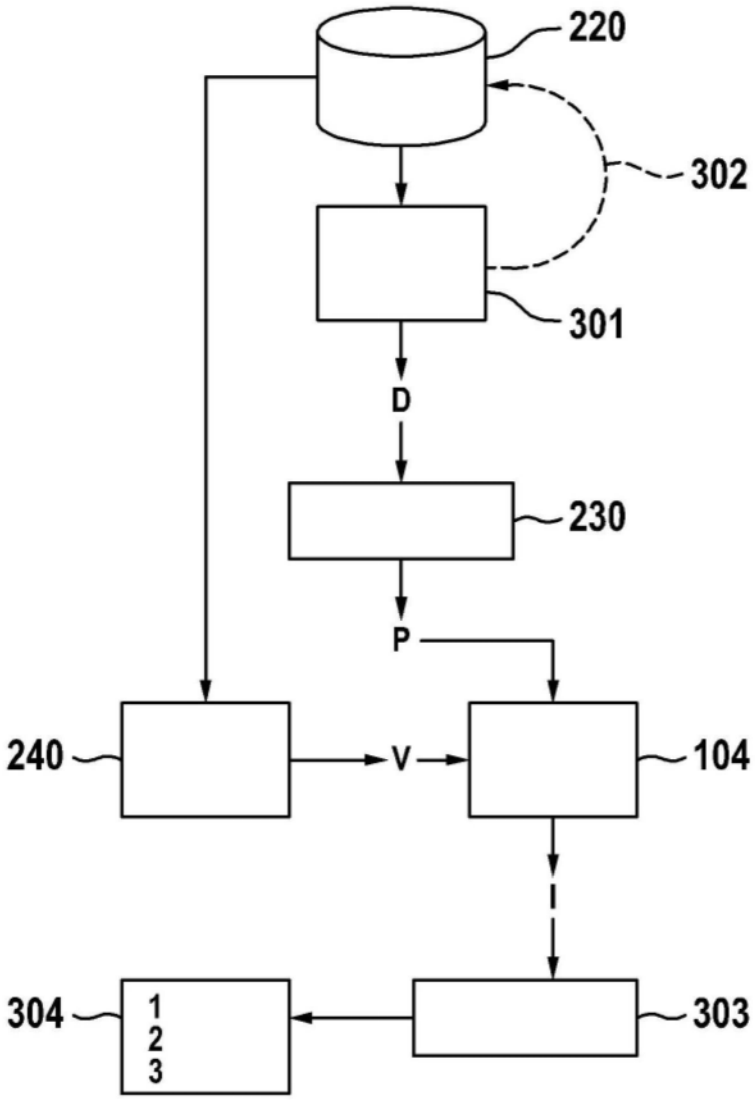


图2

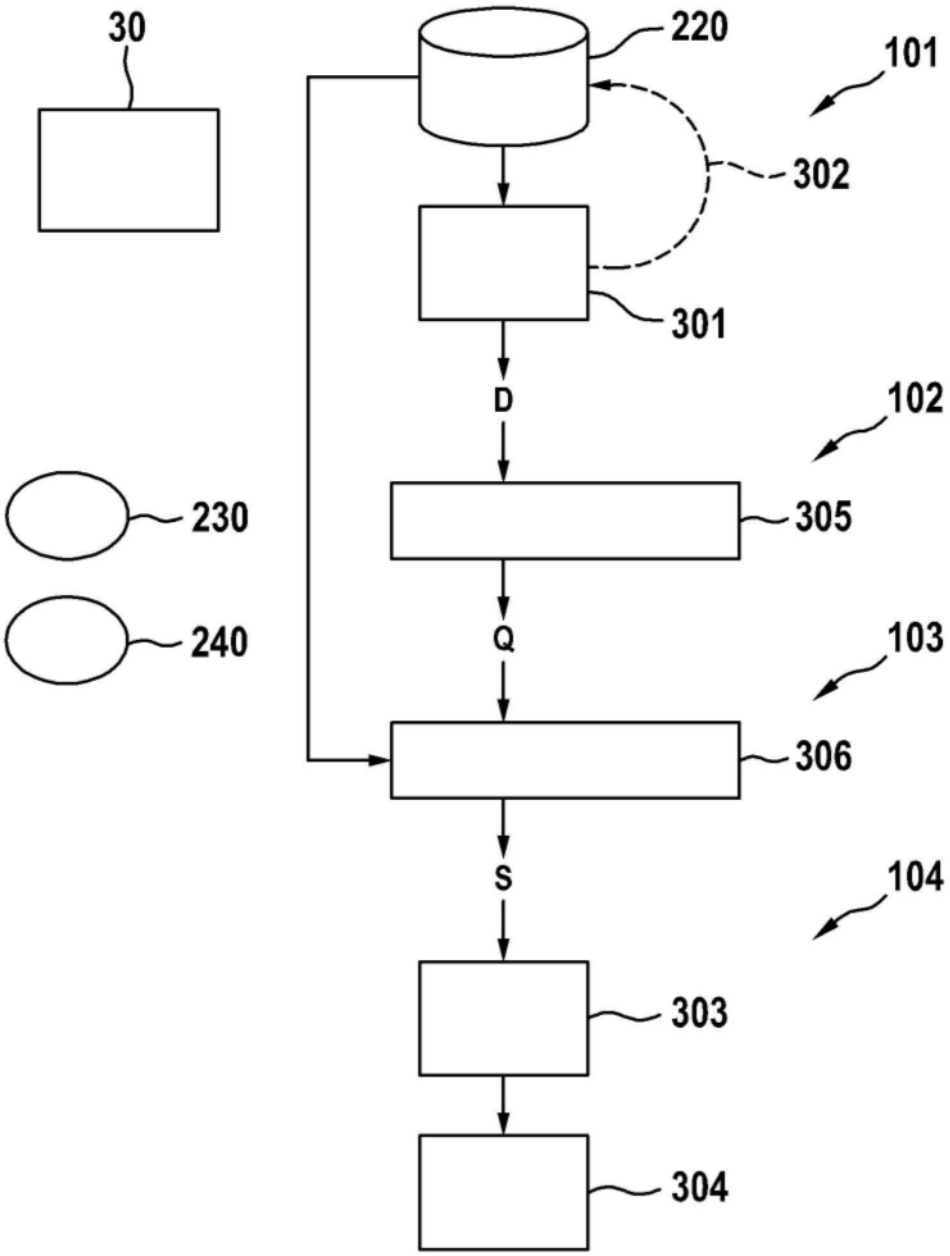


图3