(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 106561025 A
(43)申请公布日 2017.04.12

(21)申请号 201610116015.3

(22)申请日 2016.03.01

(30)优先权数据
5315/CHE/2015 2015.10.05 IN

(71)申请人 维布络有限公司
地址 印度卡纳塔克邦班加罗尔

(72)发明人 R·K·辛古如

(74)专利代理机构 上海思微知识产权代理事务所(普通合伙) 31237
代理人 智云

(51)Int.Cl.
H04L 29/06(2006.01)

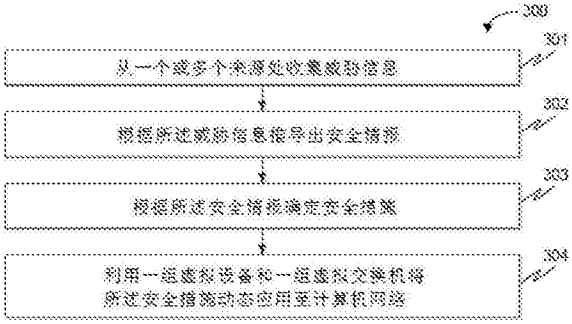
权利要求书2页 说明书8页 附图3页

(54)发明名称

用于提供计算机网络安全的系统和方法

(57)摘要

本发明公开了一种用于提供计算机网络安全的系统和方法。该方法包括:从一个或多个来源处收集威胁信息;根据所述威胁信息推导安全情报;根据所述安全情报确定安全措施;以及通过一组虚拟设备和一组虚拟交换机将所述安全措施动态应用至计算机网络。



CN 106561025 A

1.一种用于提供计算机网络安全的方法,其特征在于,该方法包括:

由一处理器从一个或多个来源处收集威胁信息;

由所述处理器根据所述威胁信息推导安全情报;

由所述处理器根据所述安全情报确定安全措施;以及

由所述处理器通过一组虚拟设备和一组虚拟交换机将所述安全措施动态应用至计算机网络。

2.如权利要求1所述的方法,其特征在于,推导安全情报包括,通过向所述威胁信息实施过滤、分析和基于声誉的试探中的至少一个,确定一个或多个潜在安全威胁。

3.如权利要求2所述的方法,其特征在于,确定安全措施包括,针对所述一个或多个潜在安全威胁中的每一个,均确定对应的安全措施。

4.如权利要求1所述的方法,其特征在于,还包括根据所述安全情报触发警报。

5.如权利要求1所述的方法,其特征在于,所述动态应用包括,将所述安全措施映射至所述一组虚拟设备和所述一组虚拟交换机。

6.如权利要求5所述的方法,其特征在于,所述动态应用包括,根据所述映射,动态部署所述一组虚拟设备。

7.如权利要求5所述的方法,其特征在于,所述动态应用包括,根据所述映射,利用多个数据包过滤器对所述一组虚拟交换机进行动态编程,以对网络业务进行导向。

8.如权利要求1所述的方法,其特征在于,所述一组虚拟设备中的每一个均为用于执行预定任务的虚拟机,而且均通过网络功能虚拟化实现。

9.如权利要求1所述的方法,其特征在于,所述一组虚拟交换机中的每一个均由软件定义网络进行编程。

10.如权利要求1所述的方法,其特征在于,所述一组虚拟设备中的每一个用于仿真防火墙、入侵预防系统、深度数据包检测及网络业务整形器中的至少一个。

11.一种用于提供计算机网络安全的系统,其特征在于,该系统包括:

至少一个处理器;以及

存有指令的计算机可读介质,所述指令在由所述至少一个处理器执行时使得该至少一个处理器执行操作,该操作包括:

从一个或多个来源处收集威胁信息;

根据所述威胁信息推导安全情报;

根据所述安全情报确定安全措施;以及

通过一组虚拟设备和一组虚拟交换机将所述安全措施动态应用至计算机网络。

12.如权利要求11所述的系统,其特征在于,推导安全情报包括,通过向所述威胁信息实施过滤、分析和基于声誉的试探中的至少一个,确定一个或多个潜在安全威胁。

13.如权利要求12所述的系统,其特征在于,确定安全措施包括,针对所述一个或多个潜在安全威胁中的每一个,均确定对应的安全措施。

14.如权利要求11所述的系统,其特征在于,所述动态应用包括,将所述安全措施映射至所述一组虚拟设备和所述一组虚拟交换机。

15.如权利要求14所述的系统,其特征在于,所述动态应用包括:

根据所述映射,动态部署所述一组虚拟设备;以及

根据所述映射，利用多个数据包过滤器对所述一组虚拟交换机进行动态编程，以对网络业务进行导向。

16.如权利要求11所述的系统，其特征在于，所述一组虚拟设备中的每一个均为用于执行预定任务的虚拟机，均通过网络功能虚拟化实现，而且用于仿真防火墙、入侵预防系统、深度数据包检测及网络业务整形器中的至少一个。

17.如权利要求11所述的系统，其特征在于，所述一组虚拟交换机中的每一个均由软件定义网络进行编程。

18.一种非暂时性计算机可读介质，该介质存有计算机可执行指令，其特征在于，所述指令用于：

从一个或多个来源处收集威胁信息；

根据所述威胁信息推导安全情报；

根据所述安全情报确定安全措施；以及

通过一组虚拟设备和一组虚拟交换机将所述安全措施动态应用至计算机网络。

用于提供计算机网络安全的系统和方法

技术领域

[0001] 本发明总体涉及计算机网络，尤其涉及一种用于提供计算机网络安全的系统和方法。

背景技术

[0002] 数字设备在最近几年变得无处不在，这些设备包括计算机、笔记本电脑、膝上型电脑、平板电脑、蜂窝电话、智能电话等。在数字化程度越来越高的当今世界上，为了实现信息交流，这些数字设备以可通信方式连接于计算机网络。计算机网络安全为计算机网络的一个重要领域，其为设计用于对计算机网络和连接于计算机网络的数字设备实施保护，以防止其遭受数字攻击和数据窃取的活动。这些活动保障了网络和数据的可用性、可靠性、完整性以及安全性。网络安全漏洞可对个人用户和企业造成严重影响。

[0003] 如今，存在多种用于提供计算机网络安全的技术。举例而言，防火墙、入侵预防系统和虚拟专用网络(VPN)等昂贵的硬件设备如今正用于处理网络安全。然而，这些硬件设备通常由于已预先配置，因此不能根据需求在运行过程中动态改变。在一些情况下，每当发现新的威胁时，可通过新的威胁特征对软件进行周期性升级。此外，为了处理多变的网络业务及负载，上述硬件设备存在过度配置的问题。因此，在将威胁信息转化为正确的安全情报方面，以及对安全情报进行准确和及时的应用方面，现有技术存在效率低下和能力有限的问题。这有可能给机构组织造成服务中断及严重经济损失的后果。

发明内容

[0004] 在一种实施方式中，本发明公开了一种用于提供计算机网络安全的方法。在一个实施例中，所述方法包括：从一个或多个来源处收集威胁信息；根据所述威胁信息推导安全情报；根据所述安全情报确定安全措施；以及通过一组虚拟设备和一组虚拟交换机将所述安全措施动态应用至计算机网络。

[0005] 在一种实施方式中，本发明还公开了一种用于提供计算机网络安全的系统。在一个实施例中，所述系统包括：至少一个处理器，以及以可通信方式连接于所述至少一个处理器的存储器。所述存储器存有处理器可执行指令，该指令在执行时使得所述处理器执行操作，该操作包括：从一个或多个来源处收集威胁信息；根据所述威胁信息推导安全情报；根据所述安全情报确定安全措施；以及通过一组虚拟设备和一组虚拟交换机将所述安全措施动态应用至计算机网络。

[0006] 在一种实施方式中，本发明还公开了一种非暂时性计算机可读介质，该介质存有用于提供计算机网络安全的计算机可执行指令。在一个实施例中，所存指令在由处理器执行时使得该处理器执行操作，该操作包括：从一个或多个来源处收集威胁信息；根据所述威胁信息推导安全情报；根据所述安全情报确定安全措施；以及通过一组虚拟设备和一组虚拟交换机将所述安全措施动态应用至计算机网络。

[0007] 应当理解的是，以上概略描述与以下详细描述均仅在于例示和说明，而不在于限

制所要求保护的发明。

附图说明

[0008] 所附各图并入本发明之内并构成本发明的一部分，用于对例示实施方式进行描述，并与说明书一道阐明所公开的原理。

[0009] 图1为根据本发明的一些实施方式用于提供计算机网络安全的例示系统的框图。

[0010] 图2为根据本发明的一些实施方式用于提供计算机网络安全的方法的概略流程图。

[0011] 图3为根据本发明的一些实施方式用于提供计算机网络安全的例示方法的流程图。

[0012] 图4为用于实施符合本发明实施方式的例示计算机系统框图。

具体实施方式

[0013] 以下，参考附图，对例示实施方式进行描述。在任何方便之处，各图中均采用相同附图标记指代相同或类似部件。虽然本文中描述了所公开原理的实施例和特征，但是在不脱离所公开实施方式的精神和范围的前提下，还可进行修改、调整以及做出其他实施方式。以下具体描述意在仅视作例示，而真正的范围及精神如下附权利要求书所述。

[0014] 现在参考图1，该图所示为根据本发明一些实施方式用于提供计算机网络安全的例示系统100。具体而言，系统100通过从各种资源中获取威胁信息，根据所述威胁信息并利用智能过滤和分析确定安全威胁(security threat)和相应的安全措施，以及通过虚拟设备和虚拟交换机将所述安全措施应用于计算机网络，在该计算机网络内实现改进的网络安全威胁检测预防技术。系统100包括威胁数据供给器101、威胁情报中心102、核心安全指导器103、虚拟协调器104以及软件定义网络(Software Defined Network,SDN)控制器105。

[0015] 威胁数据供给器101从各种来源处收集威胁相关信息。所述各种来源可包括基于众包的公共论坛106、内部或外部安全研究团队107、工具馈信108等。在一些实施方式中，工具馈信108可包括，但不限于，从已安装程序和应用生成的日志中收集信息的SPLUNK分析馈信。此外，在一些实施方式中，工具馈信108可包括来自网络业务分析器的网络业务分析。

[0016] 威胁情报中心102从各种威胁数据供给器101收集数据，并通过对威胁信息实施智能过滤和分析而推导安全情报。所述安全情报包括潜在安全威胁和相应的安全措施。该安全情报传递至核心安全指导器103，以实施自适应式威胁预防和遏制。

[0017] 核心安全指导器103为整个系统100的中央控制器。核心安全指导器103从威胁情报中心102接收所述安全情报，并通过虚拟设备109和虚拟交换机110将所述安全措施动态应用至所述计算机网络。在一些实施方式中，核心安全指导器103将所述安全情报映射至待部署的相关虚拟设备109，以及映射至用于对相关虚拟交换机110进行编程的相关数据包过滤器。其后，核心安全指导器103将所述映射传递至虚拟协调器104。此外，在一些实施方式中，核心安全指导器103可根据所述安全情报触发警报。

[0018] 虚拟协调器104可以为专用协调器，或者OpenStack™等现有协调器之一。虚拟协调器104包括两个主要模块，即配置模块111和过滤模块112。配置模块111在运行中对各种虚拟设备(如VA1、VA2和VA3)109进行动态部署(即实例化或删除)，并根据上述映射以及具体

需求，利用服务链对所述各种虚拟设备进行连接。每个虚拟设备109均为用于执行预定任务的虚拟机，而且均通过网络功能虚拟化实现。虚拟设备109类似于防火墙、入侵预防系统(IPS)、深度数据包检测(DPI)、网络业务整形器等。此外，根据上述映射，过滤模块112通过SDN控制器105和各种数据包过滤器对各种虚拟交换机(如VS1、VS2和VS3)110进行编程，以实现网络业务的正确导向。每个虚拟交换机110均由软件定义网络编程。

[0019] 所述SDN控制器105包括北向应用编程接口(API)模块113、控制器114以及南向API模块115。北向API模块113使用虚拟协调器104提供的所述过滤器并对所述虚拟交换机进行动态编程，以将网络业务从来源处116导向至目的地117。所述动态编程由南向API模块115通过Open Flow、NETCONF、XMPP等各种南向协议实现。

[0020] 在操作中，系统100从外部安全机构、众包、内部研究团队、工具馈信等各种来源处收集威胁信息。其后，系统100通过智能过滤和分析将所收集的威胁信息转化为相关安全情报。该安全情报识别出潜在的安全威胁以及相应的安全措施。根据所识别的威胁和相应措施，系统100对虚拟设备(利用网络功能虚拟化)进行动态部署，并对必要的虚拟交换机进行编程(利用软件定义网络)。编程后的交换机将可疑业务定向至另一信道，其中，该另一信道部署有可采取预防措施的适当虚拟设备。系统100还可设置为当检测到任何安全威胁时触发预定类型的警报，以对用户或管理员进行通知。

[0021] 应当注意的是，系统100可在可编程门阵列、可编程阵列逻辑、可编程逻辑器件等可编程硬件设备内实现。或者，系统100也可在由各种类型处理器执行的软件内实现。被认定的可执行代码引擎例如可包括计算机指令的一个或多个例如组织为对象、程序、功能、模块或其他构建体的物理或逻辑块。然而，在物理形式上，被认定引擎的可执行代码无需位于一处，而是可包括存于不同位置处的不同指令，当这些指令在逻辑上相互接合时，可构成所述引擎并实现该引擎的标称目的。实际上，可执行代码引擎可以为单个指令或多个指令，而且甚至可分布于不同应用程序的多个不同代码段上以及可分布于多个存储器装置上。

[0022] 现在参考图2，该图所示为根据本发明的一些实施方式用于提供计算机网络安全的例示方法200的概略流程图。方法200包括，步骤201：从各种来源处获取威胁信息；步骤202：确定安全威胁和相应的预防措施；步骤203：利用虚拟设备和虚拟交换机执行所述预防措施。以下，对这些步骤当中的每个步骤进行更加详细的描述。

[0023] 在步骤201中，由所述威胁数据供给模块从内部或外部安全研究团队、工具馈信、众包等各种资源中获取或收集威胁信息。在一些实施方式中，所述来源可包括，但不限于，网络监控(具体为社交网络监控)、垃圾邮件捕捉器、诱捕蜜罐、针对恶意软件和漏洞利用代码的链接爬行等。之后，如上所述，威胁数据供给器所获取的信息被提供于威胁情报中心，用于进一步处理。

[0024] 在步骤202中，所述威胁情报中心根据获取自各种资源处的不同格式和不同标准的威胁信息生成合并的标准化威胁信息。提供至所述威胁情报中心的威胁信息包括已分析且获取自多个来源以生成有助于安全威胁预防的见解的信息。本领域技术人员可理解的是，不同来源所提供的威胁信息具有不同格式和不同标准。例如，基于SPLUNK工具的信息可以为JavaScript对象表示法(JSON)格式，而众包威胁信息可以为具有逗号分隔值(CSV)格式的键值对形式。因此，为了后续使用，这些威胁信息中的每一种均转化为同一种标准格式(如XML架构)。所述标准格式描述了各种威胁的技术特征，例如已知威胁、攻击者的攻击方

法，或者其他此类证据。

[0025] 在此之后，所述威胁情报中心向所述合并的标准化威胁信息实施智能过滤、分析或基于声誉的试探，以推导出安全情报。在一些实施方式中，对所述安全情报的推导还包括：对可提供最有价值且具有与应用了相关技术的组织机构的垂直产业背景相符的最佳覆盖度的正确来源进行识别。所述分析有助于对事件进行情境化和关联，而所述基于声誉的试探有助于对所述信息来源进行排序，从而确保消除虚假或不相关的威胁信息。举例而言，在零售行业中，潜在威胁的种类可以为“拒绝服务”攻击，该攻击使得零售业客户无法在线访问相关商店。此外，所述潜在威胁还可以为对信用卡信息等客户相关机密信息进行全部或部分窃取。类似地，在医疗保健行业，所述威胁可以为窃取或操纵患者健康记录。实施分析有助于对任何安全威胁的严重性进行实况化。此外，与公共论坛相比，来自政府机构的威胁信息在声誉上可具有更高的排名。此类基于声誉的试探有助于将虚假或不严重的威胁与真正的严重威胁快速区分开来。

[0026] 在此之后，所述威胁情报中心确定出相应的预防或安全措施。这些措施为针对每个识别出的真正威胁的可执行漏洞响应和风险缓解策略。例如，所述可执行响应可以为“对来自特定来源或特定目的地的所有数据包进行阻止”，“将所有数据包转流至某特定TCP端口，以用于后续分析”，“删除被感染文件”，“对受影响的注册表项进行重写”等。

[0027] 所述核心安全指导器接收所述安全措施，并将这些措施映射至所述一组相关虚拟设备以及所述一组相关虚拟交换机。在一些实施方式中，对所述一组相关虚拟设备以及所述一组相关虚拟交换机的映射包括：根据待应用的安全措施，生成合适的数据包过滤器和虚拟设备。所述可执行漏洞响应实施为以下形式：带操作的数据包过滤器；以及虚拟设备。数据包过滤器为基于通用正则表达式的模式匹配过滤器。举例而言，简单的过滤器可以为“来自特定源地址的任何数据包”。上述虚拟协调器通过Open Flow等标准协议将这些应用至所述虚拟交换机(VS1、VS2和VS3等)。所述虚拟交换机将所有流经该虚拟交换机的数据包均利用此类过滤器进行过滤，并对其实施数据包阻截和数据包转流等上述给定操作。此外，所述虚拟设备为用于执行特定任务的预配置软件虚拟机，而且可以在运行过程中动态生成。例如，可生成用于实施深度数据包分析的虚拟设备。

[0028] 在步骤203中，所述核心安全指导器通过相关虚拟设备和虚拟交换机将所述安全措施动态应用至所述计算机网络。所述核心安全指导器与所述虚拟协调器和SDN控制器共同在所述计算机网络内执行所述预防性安全措施。网络功能虚拟化和软件定义网络共同为所需虚拟设备在运行过程中的动态生成和部署以及为相关操作在流经所述虚拟设备的业务上的实施提供了灵活性。所述SDN控制器通过合适的数据包过滤器对所述虚拟交换机进行编程，以对可疑和非可疑网络业务进行正确的导向(例如，将非可疑业务与可疑业务分离)。所述虚拟协调器对所述相关虚拟设备进行部署和配置。例如，可将可疑业务转流至专用虚拟设备(VA1、VA2和VA3等)，以用于进一步分析。

[0029] 本领域技术人员可以理解的是，有多种方法可用于提供计算机网络安全。例如，例示系统100可通过本文所述方法用于提供计算机网络安全。具体而言，本领域技术人员可以理解的是，用于实施本文所述技术和步骤的控制逻辑和/或自动化程序可由系统100通过硬件、软件或硬件及软件的组合而实现。例如，系统100内的一个或多个处理器可对合适的代码进行访问和执行，以实现本文所述的部分或所有技术。类似地，系统100内的所述一个或

多个处理器内还可纳入用于实施本文所述的部分或所有方法的专用集成电路(ASIC)。

[0030] 例如,现在参考图3,该图所示为根据本发明的一些实施方式用于利用系统100等系统提供计算机网络安全的例示控制逻辑300的流程图。如该流程图所述,控制逻辑300包括,步骤301:从一个或多个来源处收集威胁信息;步骤302:根据所述威胁信息推导出安全情报;步骤303:根据所述安全情报确定安全措施;步骤304:利用一组虚拟设备和一组虚拟交换机将所述安全措施动态应用至计算机网络。在一些实施方式中,控制逻辑300还包括根据所述安全情报触发警报的步骤。

[0031] 应当注意的是,每个虚拟设备均为用于执行预定任务的虚拟机,而且均通过网络功能虚拟化实现。此外,每个虚拟设备均类似于防火墙、入侵预防系统(IPS)、深度数据包检测(DPI)以及网络业务整形器中的至少一个。此外,每个虚拟交换机均由软件定义网络编程。

[0032] 在一些实施方式中,步骤302中对所述安全情报的推导包括,通过向所述威胁信息实施过滤、分析和基于声誉的试探中的至少一个,确定一个或多个潜在安全威胁。此外,在一些实施方式中,在步骤303中确定所述安全措施包括,针对所述一个或多个潜在安全威胁中的每一个,均确定相应的安全措施。另外,在一些实施方式中,步骤304中的动态应用包括,将所述安全措施映射至所述一组虚拟设备和所述一组虚拟交换机。在一些实施方式中,步骤304中的动态应用还包括,根据所述映射,动态部署所述一组虚拟设备。除此之外,在一些实施方式中,步骤304中的动态应用包括,根据所述映射并通过多个数据包过滤器,对所述一组虚拟交换机进行动态编程,以对网络业务进行导向。

[0033] 还应理解的是,上述技术可采用如下形式:计算机或控制器实现的方法;以及用于实施这些方法的装置。本发明还可以以含有指令的计算机程序代码的形式实施,所述指令包含于软盘、CD-ROM、硬盘驱动器或其他任何计算机可读存储介质等有形介质中,其中,当所述计算机程序代码载入计算机或控制器内并由该计算机或控制器执行时,所述计算机即成为一种用于实施本发明的装置。本发明还可以以计算机程序代码或信号的形式实施,所述计算机程序代码或信号例如存储于存储介质中,或者载入计算机或控制器内并由该计算机或控制器执行,或者经电线或电缆、光纤或电磁辐射等传输介质传输,其中,当所述计算机程序代码载入计算机内并由该计算机执行时,所述计算机即成为一种用于实施本发明的装置。当在通用微处理器中实施时,所述计算机程序代码的代码段对所述微处理器进行配置,以创建出特定的逻辑电路。

[0034] 上述公开的方法和系统可在个人计算机(PC)或服务器计算机等常规或通用计算机系统内实施。现在参考图4,该图所示为用于实施符合本发明实施方式的例示计算机系统401的框图。计算机系统401的各种变形可用于实现用于提供计算机网络安全的系统100。计算机系统401可包括中央处理单元(“CPU”或“处理器”)402。处理器402可包括至少一个用于执行程序组件的数据处理器,所述程序组件用于执行用户或系统生成的请求。用户可包括使用设备(例如,本发明范围内的设备)的个人或此类设备本身。所述处理器可包括专用处理单元,例如集成系统(总线)控制器、存储器管理控制单元、浮点单元、图形处理单元、数字信号处理单元等。所述处理器可包括微处理器,例如AMD速龙(Athlon)、毒龙(Duron)或皓龙(Opteron),ARM应用处理器,嵌入式或安全处理器,IBM PowerPC,Intel Core、安腾(Itanium)、至强(Xeon)、赛扬(Celeron)或其他处理器产品线等。处理器402可通过主机、分

布式处理器、多核、并行、网格或其他架构实现。一些实施方式可使用专用集成电路(ASIC)、数字信号处理器(DSP)、现场可编程门阵列(FPGA)等嵌入式技术。

[0035] 处理器402可配置为通过输入/输出(I/O)接口403与一个或多个I/O设备进行通信。I/O接口403可采用通信协议/方法,例如但不限于,音频、模拟、数字、单声道、RCA、立体声、IEEE-1394、串行总线、通用串行总线(USB)、红外、PS/2、BNC、同轴、组件、复合、数字视觉接口(DVI)、高清晰度多媒体接口(HDMI)、射频天线、S-视频,VGA、IEEE 802.n/b/g/n/x、蓝牙、蜂窝(例如码分多址(CDMA)、高速分组接入(HSPA+)、移动通信全球系统(GSM)、长期演进(LTE)、WiMax等)等。

[0036] 通过使用I/O接口403,计算机系统401可与一个或多个I/O设备进行通信。举例而言,输入设备404可以为天线、键盘、鼠标、操纵杆、(红外)遥控、摄像头、读卡器、传真机、加密狗、生物计量阅读器、麦克风、触摸屏、触摸板、轨迹球、传感器(例如加速度计、光传感器、GPS、陀螺仪、接近传感器等)、触控笔、扫描仪、存储设备、收发器、视频设备/视频源、头戴式显示器等。输出设备405可以为打印机、传真机、视频显示器(例如阴极射线管(CRT)、液晶显示器(LCD)、发光二极管(LED)、等离子等)、音频扬声器等。在一些实施方式中,收发器406可与处理器402连接。所述收发器可促进各类无线传输或接收。例如,所述收发器可包括以可操作方式连接至收发器芯片(例如德州仪器(Texas Instruments)WiLink WL1283、博通(Broadcom)BCM4750IUB8、英飞凌科技(Infineon Technologies)X-Gold 618-PMB9800等)的天线,以实现IEEE 802.11a/b/g/n、蓝牙、频率调制(FM)、全球定位系统(GPS)、2G/3G HSDPA/HSUPA通信等。

[0037] 在一些实施方式中,处理器402可配置为通过网络接口407与通信网络408进行通信。网络接口407可与通信网络408通信。所述网络接口可采用连接协议,包括但不限于,直接连接、以太网(例如双绞线10/100/1000BaseT)、传输控制协议/网际协议(TCP/IP)、令牌环、IEEE 802.11a/b/g/n/x等。通信网络408可包括,但不限于,直接互连、局域网(LAN)、广域网(WAN)、无线网络(例如使用无线应用协议)、因特网等。通过网络接口407和通信网络408,计算机系统401可与设备410、411和412通信。这些设备可包括,但不限于,个人计算机、服务器、传真机、打印机、扫描仪以及各种移动设备,例如蜂窝电话、智能电话(例如苹果手机(AppleiPhone)、黑莓手机(Blackberry)、基于安卓(Android)系统的电话等)、平板电脑、电子书阅读器(亚马逊(Amazon)Kindle,Nook等)、膝上型计算机、笔记本电脑、游戏机(微软(Microsoft)Xbox、任天堂(Nintendo)DS,索尼(Sony)PlayStation等)等。在一些实施方式中,计算机系统401可本身包含一个或多个上述设备。

[0038] 在一些实施方式中,处理器402可配置为通过存储接口412与一个或多个存储设备(例如RAM 413、ROM 414等)进行通信。所述存储接口可采用串行高级技术连接(SATA)、集成驱动电子设备(IDE)、IEEE 1394、通用串行总线(USB)、光纤通道、小型计算机系统接口(SCSI)等连接协议连接至存储设备,该存储设备包括,但不限于,存储驱动器、可移除磁盘驱动器等。所述存储驱动器还可包括磁鼓、磁盘驱动器、磁光驱动器、光盘驱动器、独立磁盘冗余阵列(RAID)、固态存储设备、固态驱动器等。

[0039] 所述存储设备可存储一系列程序或数据库组件,包括但不限于,操作系统416、用户界面417、网页浏览器418、邮件服务器419、邮件客户端420、用户/应用程序数据421(例如本发明中所述的任何数据变量或数据记录)等。操作系统416可促进计算机系统401的资源

管理和运行。操作系统例如包括，但不限于，苹果Macintosh OS X、Unix、类Unix系统套件(例如伯克利软件套件(BSD)、FreeBSD、NetBSD、OpenBSD等)、Linux套件(如红帽(Red Hat)、Ubuntu、Kubuntu等)、IBM OS/2、微软Windows(XP，Vista/7/8等)、苹果iOS、谷歌(Google)安卓、黑莓操作系统等。用户界面417可利用文本或图形工具促进程序组件的显示、执行、互动、操控或操作。例如，用户界面可在以可操作方式连接至计算机系统401的显示系统上提供计算机交互界面元件，如光标、图标、复选框、菜单、滚动条、窗口、窗口部件等。还可采用图形用户界面(GUI)，包括但不限于，苹果Macintosh操作系统的Aqua、IBM OS/2、微软Windows(例如Aero、Metro等)、Unix X-Windows、网页界面库(例如ActiveX、Java、Javascript、AJAX、HTML、Adobe Flash等)等。

[0040] 在一些实施方式中，计算机系统401可执行网页浏览器418存储的程序组件。所述网页浏览器可以为超文本浏览应用程序，如微软网络探路者(Internet Explorer)、谷歌浏览器(Chrome)、谋智火狐(MozillaFirefox)、苹果浏览器(Safari)等。安全网页浏览可通过HTTPS(安全超文本传输协议)、安全套接字层(SSL)、安全传输层(TLS)等实现。网页浏览器可使用AJAX、DHTML、Adobe Flash、JavaScript、Java、应用程序编程接口(API)等工具。在一些实施方式中，计算机系统401可执行邮件服务器419存储的程序组件。所述邮件服务器可以为微软Exchange等因特网邮件服务器。所述邮件服务器可使用ASP、ActiveX、ANSI C++/C#、微软.NET、CGI脚本、Java、JavaScript、PERL、PHP、Python、WebObjects等工具。所述邮件服务器还可使用因特网信息访问协议(IMAP)、邮件应用程序编程接口(MAPI)、微软Exchange、邮局协议(POP)、简单邮件传输协议(SMTP)等通信协议。在一些实施方式中，计算机系统401可执行邮件客户端420存储的程序组件。所述邮件客户端可为苹果Mail、微软Entourage、微软Outlook、谋智Thunderbird等邮件查看程序。

[0041] 在一些实施方式中，计算机系统401可存储用户/应用程序数据421，例如本发明中所述数据、变量、记录等(如威胁信息、安全威胁、安全措施、数据包过滤器、虚拟设备、虚拟交换机等)。此类数据库可以为容错、关系、可扩展、安全数据库，例如甲骨文(Oracle)或赛贝斯(Sybase)。或者，上述数据库可通过数组、散列、链表、结构、结构化文本文件(例如XML)、表格等标准化数据结构实现，或者实施为面向对象的数据库(例如通过ObjectStore、Poet、Zope等)。上述数据库可以为合并或分布数据库，有时分布于本发明所讨论的上述各种计算机系统之间。应该理解的是，可以以任何可工作的组合形式对上述任何计算机或数据库组件的结构及操作进行组合、合并或分布。

[0042] 本领域技术人员可以理解的是，上述各种实施方式中所述的技术用于提供高效和高性价比的动态计算机网络安全。通过对网络功能虚拟化、软件定义网络和高级威胁情报的综合利用，上述技术以高性价比的方式实现了改进的主动网络安全威胁检测预防。此外，通过对正确安全情报的实时推导，并利用合适的虚拟设备和虚拟交换机将合适的预防措施及时应用至所述计算机网络，所述技术还实现了对来自多个可靠来源的威胁情报交流中各种进展的利用。另外，所述技术还用于按照网络业务负载动态扩大或缩小需使用硬件的规模。除此之外，如本领域技术人员可以理解的，上述各种实施方式中所述的技术可部署于客户端，或以服务的形式提供。此外，所述技术可配置为对客户的现有威胁数据供给器和分析数据进行使用。

[0043] 本说明书已对用于提供计算机网络安全的系统和方法进行了描述。所示步骤用于

说明所述例示实施方式，并且应当预想到的是，随着技术的不断发展，特定功能的执行方式也将发生改变。本文所呈现的上述实施例用于说明而非限制目的。此外，为了描述的方便性，本文对各功能构建模块边界的定义为任意性的，只要其上述功能及其关系能够获得适当执行，也可按其他方式定义边界。根据本申请的启示内容，替代方案(包括本申请所述方案的等同方案、扩展方案、变形方案、偏差方案等)对于相关领域技术人员是容易理解的。这些替代方案均落入所公开实施方式的范围和精神内。

[0044] 此外，一个或多个计算机可读存储介质可用于实施本发明的实施方式。计算机可读存储介质是指可对处理器可读取的信息或数据进行存储的任何类型的物理存储器。因此，计算机可读存储介质可对由一个或多个处理器执行的指令进行存储，包括用于使处理器执行根据本申请实施方式的步骤或阶段的指令。“计算机可读介质”一词应理解为包括有形物件且不包括载波及瞬态信号，即为非暂时性介质，例如随机存取存储器(RAM)、只读存储器(ROM)、易失性存储器、非易失性存储器、硬盘驱动器、只读光盘存储器(CD-ROM)、DVD、闪存驱动器、磁盘以及其他任何已知物理存储介质。

[0045] 以上发明及实施例旨在于仅视为示例性内容及实施例，所公开实施方式的真正范围和精神由以下权利要求指出。

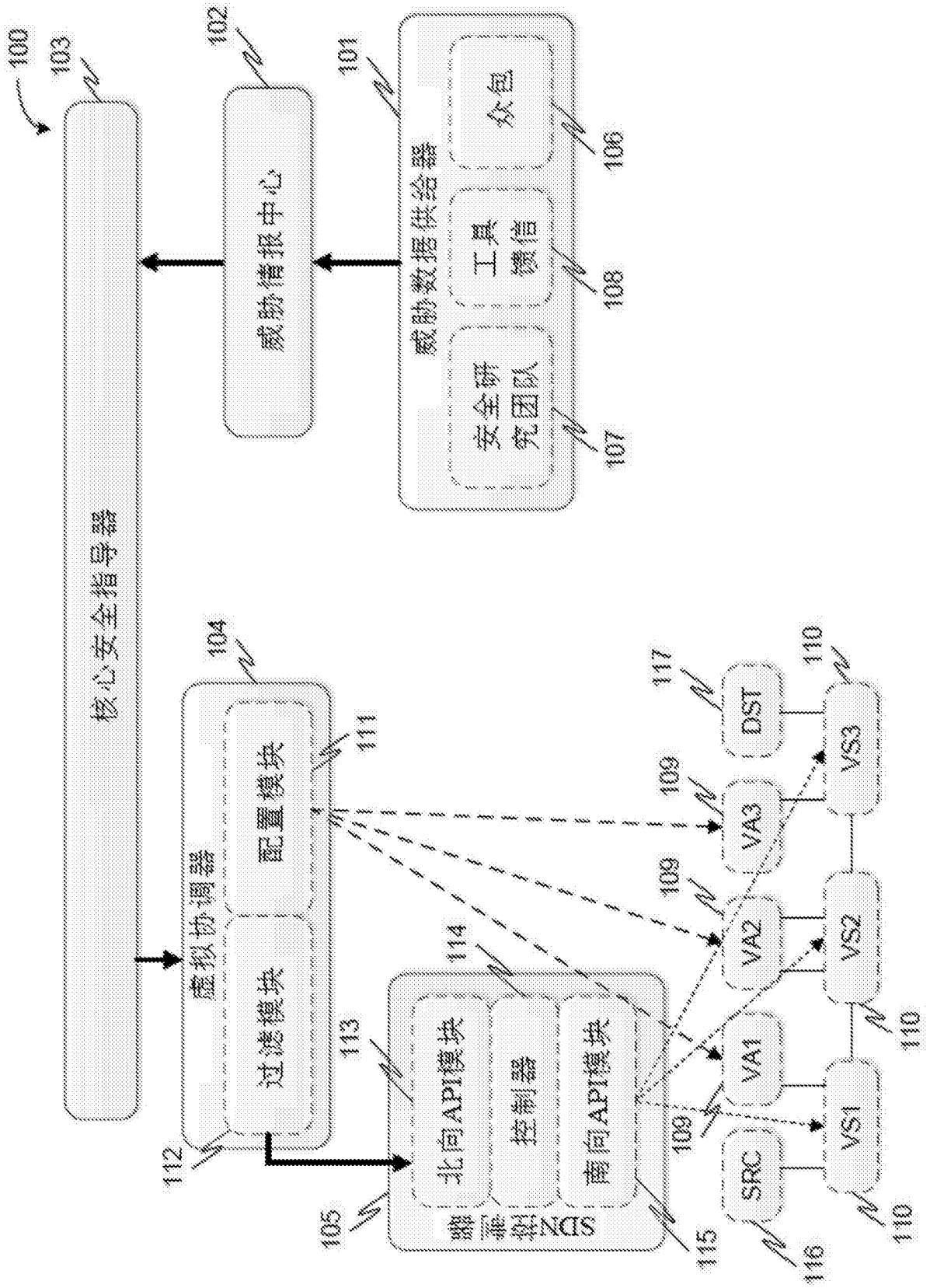

核心安全指导器
威胁情报中心
威胁数据供给器
众包
工具情报
安全研究团队
虚拟协调器
配置模块
过滤模块
SDN控制器
北向API模块
控制器
南向API模块
VA1
VA2
VA3
VS1
VS2
VS3
SRC
DST
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117

图1

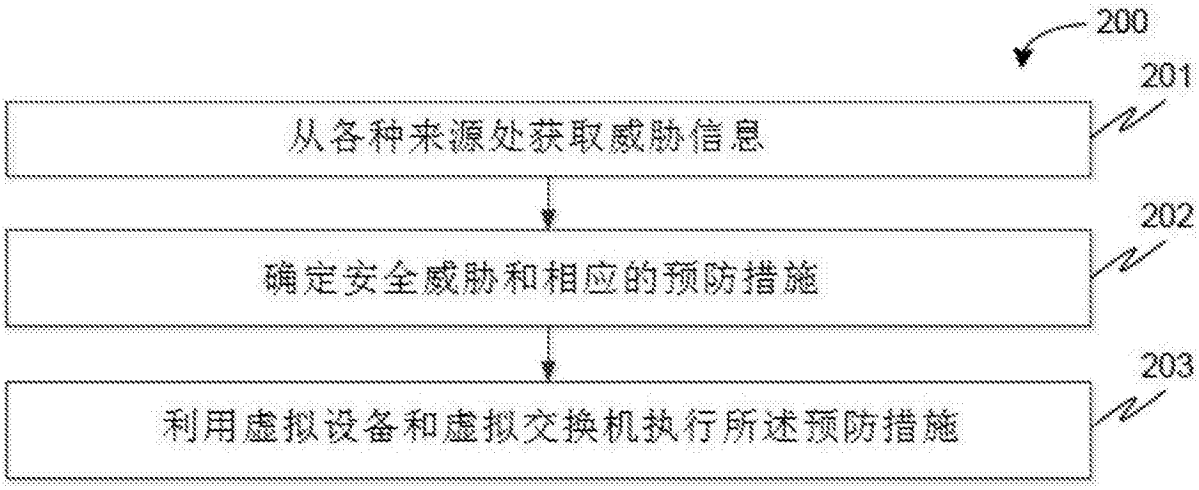

200
201
从各种来源处获取威胁信息
202
确定安全威胁和相应的预防措施
203
利用虚拟设备和虚拟交换机执行所述预防措施

图2

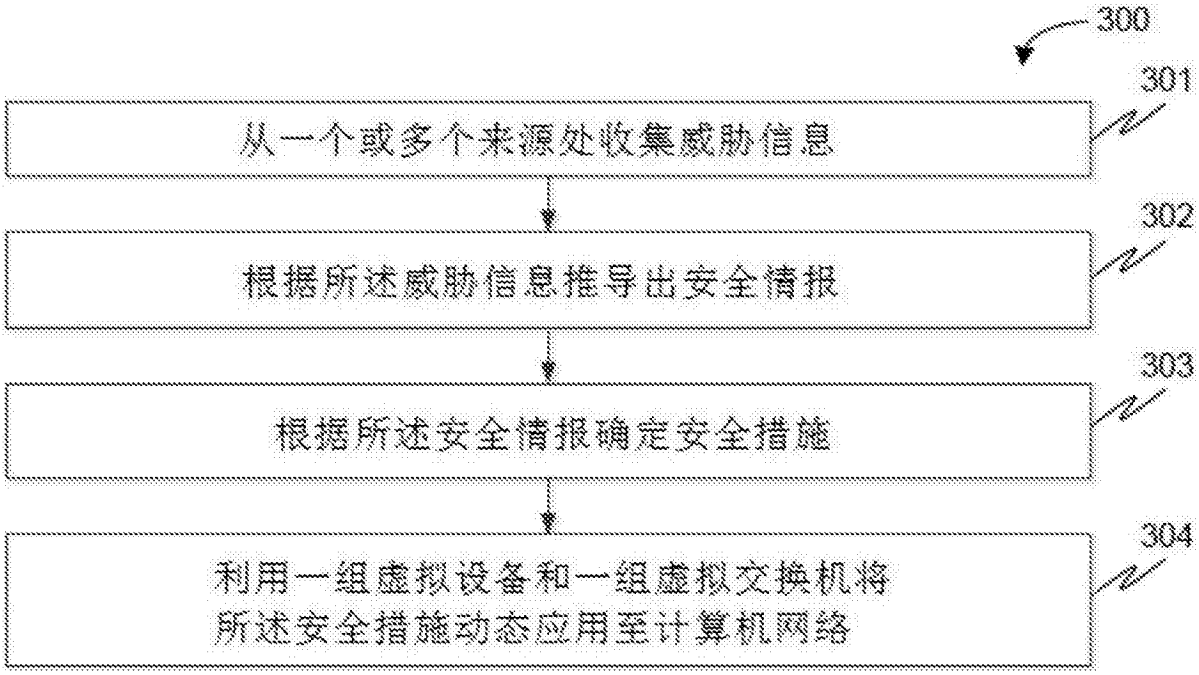

300
301
从一个或多个来源处收集威胁信息
302
根据所述威胁信息推导出安全情报
303
根据所述安全情报确定安全措施
304
利用一组虚拟设备和一组虚拟交换机将
所述安全措施动态应用至计算机网络

图3

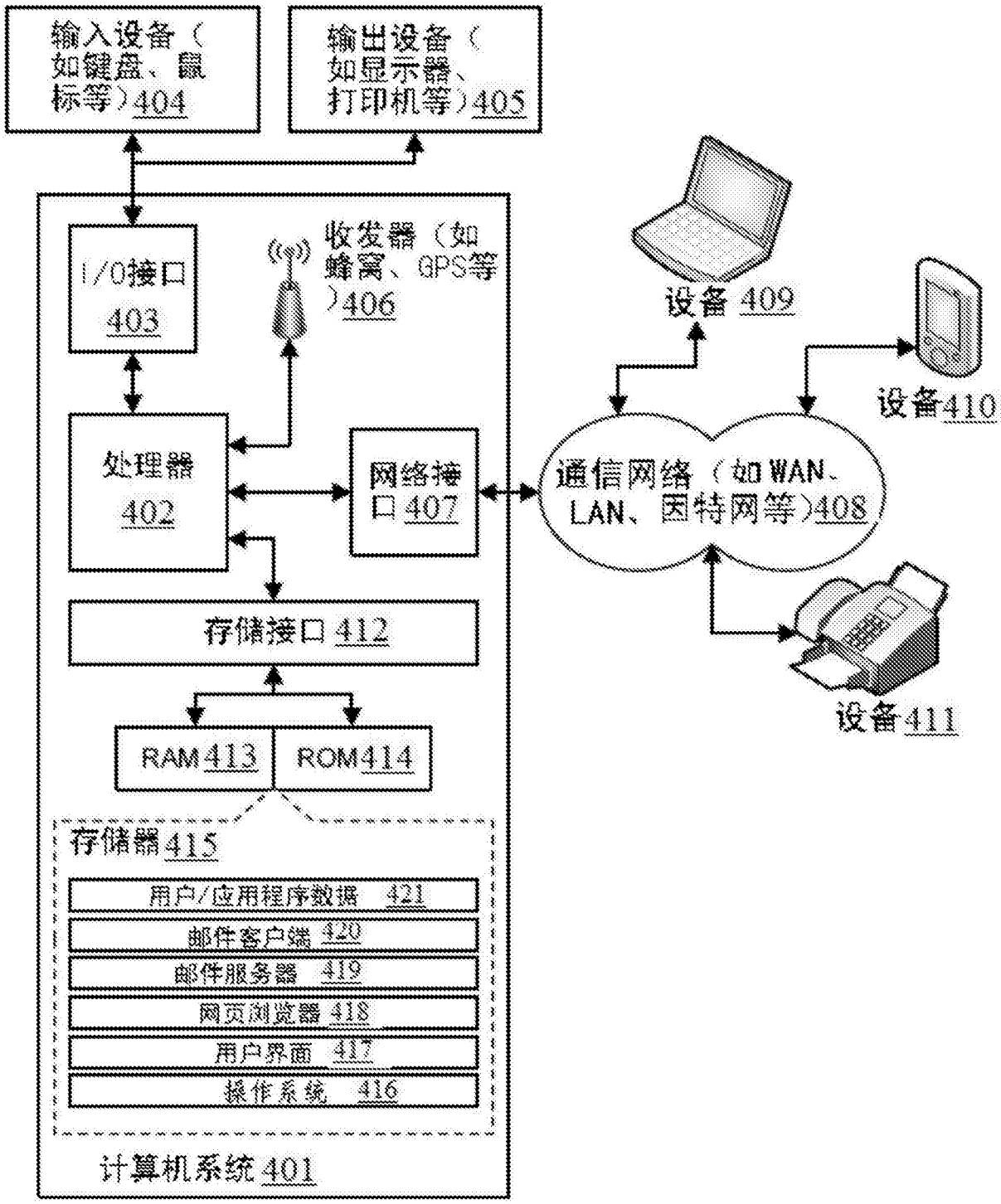

输入设备（如键盘、鼠标等）404
输出设备（如显示器、打印机等）405
I/O接口 403
收发器（如蜂窝、GPS等）406
处理器 402
网络接口 407
存储接口 412
RAM 413
ROM 414
存储器 415
用户/应用程序数据 421
邮件客户端 420
邮件服务器 419
网页浏览器 418
用户界面 417
操作系统 416
计算机系统 401
设备 409
设备 410
通信网络（如 WAN、LAN、因特网等）408
设备 411

图4