(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111885007 B
(45)授权公告日 2023.03.24

(21)申请号 202010612437.6

(22)申请日 2020.06.30

(65)同一申请的已公布的文献号
申请公布号 CN 111885007 A

(43)申请公布日 2020.11.03

(73)专利权人 北京长亭未来科技有限公司
地址 100024 北京市朝阳区管庄东里(朝阳区副食品公司)3幢1层B26

(72)发明人 刘超 龚潇 刘亚光 陈彪 罗晶晶 张子墨 贾悦霖 王大鼎 赵凡 刘玉仙 王江涛 张嘉欢

(74)专利代理机构 深圳睿臻知识产权代理事务所(普通合伙) 44684
专利代理师 张海燕

(51)Int.Cl.
*H04L 9/40*(2022.01)

(56)对比文件
JP 2003298652 A,2003.10.17
CN 108260186 A,2018.07.06
US 2018367548 A1,2018.12.20
WO 2010011182 A2,2010.01.28

审查员 张伟

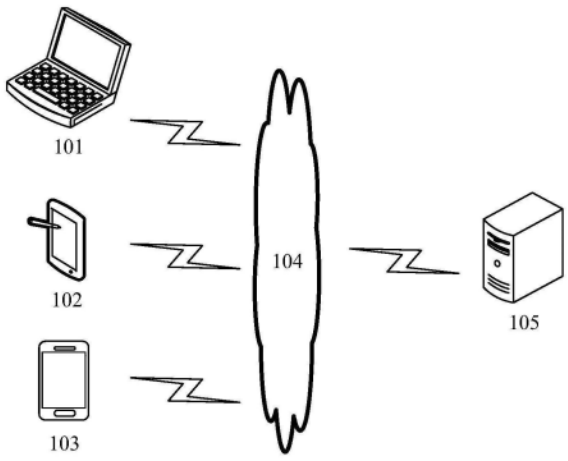
权利要求书3页 说明书10页 附图5页

(54)发明名称

信息溯源方法、装置、系统及存储介质

(57)摘要

本申请公开的实施例公开了信息溯源方法、装置、系统及存储介质。该方法的一具体实施方式包括:响应于接收到客户端发送的访问请求,生成与客户端相对应的标识信息并发送该标识信息至客户端;获取该标识信息对应的行为日志;根据该标识信息和行为日志,确定客户端的身份信息。该实施方式实现了在降低资源占用的同时更加隐蔽地实现攻击者身份信息的追踪溯源。




CN 111885007 B

1.一种信息溯源方法,其特征在于,包括:

响应于接收到客户端发送的访问请求,生成与所述客户端相对应的标识信息并发送所述标识信息至所述客户端;

获取所述标识信息对应的行为日志;

根据所述标识信息和所述行为日志,确定所述客户端的身份信息;

所述方法还包括:预先设置信息接收节点;

利用所述信息接收节点采集所述标识信息以及溯源信息;

所述响应于接收到客户端发送的访问请求,生成与所述客户端相对应的标识信息并发送所述标识信息至所述客户端,具体包括:

响应于接收到客户端发送的访问请求,所述信息接收节点检测多个域的任意域中是否已存在与所述客户端对应的标识信息;

响应于不存在,所述信息接收节点生成与所述客户端对应的标识信息并发送所述标识信息至所述客户端;

响应于存在,所述信息接收节点发送所述标识信息至所述客户端。

2.根据权利要求1所述的信息溯源方法,其特征在于,所述方法还包括:

响应于接收到客户端发送的访问请求,获取所述客户端的溯源信息;以及

所述根据所述标识信息和所述行为日志,确定所述客户端的身份信息,具体包括:

根据所述标识信息、溯源信息和所述行为日志,确定所述客户端的身份信息。

3.根据权利要求2所述的信息溯源方法,其特征在于,预先设置蜜罐系统,所述方法还包括:

响应于所述客户端访问所述蜜罐系统,所述蜜罐系统执行所述生成所述标识信息以及获取所述行为日志、所述溯源信息的步骤;

以及,所述蜜罐系统执行所述生成标识信息的步骤,具体包括:

所述蜜罐系统根据蜜罐系统自身标识生成所述标识信息,以及将所述标识信息发送至所述客户端。

4.根据权利要求1所述的信息溯源方法,其特征在于,预先设置真实业务系统,所述方法还包括:

响应于所述客户端访问所述真实业务系统,所述真实业务系统执行所述生成标识信息以及获取所述行为日志的步骤;

以及,所述真实业务系统执行所述生成标识信息的步骤,具体包括:

所述真实业务系统根据真实业务系统自身标识生成所述标识信息,以及将所述标识信息发送至所述客户端。

5.根据权利要求1所述的信息溯源方法,其特征在于,所述响应于接收到客户端发送的访问请求,生成与所述客户端相对应的标识信息并发送所述标识信息至所述客户端,具体包括:

响应于接收到客户端发送的访问请求,检测所述客户端是否存在攻击行为;

响应于存在攻击行为,生成与所述客户端对应的标识信息并发送所述标识信息至所述客户端,以及根据所述客户端的攻击行为,对所述客户端进行分类。

6.根据权利要求1所述的信息溯源方法,其特征在于,所述方法还包括:

响应于再次接收到所述客户端发送的访问请求，查询所述客户端是否存储有与其相对应的标识信息；

响应于所述客户端未存储有所述标识信息，生成与所述客户端相对应的标识信息并发送所述标识信息至所述客户端。

7.根据权利要求1-6中任一项所述的信息溯源方法，其特征在于，所述根据所述标识信息和所述行为日志，确定所述客户端的身份信息，具体包括：

根据多个所述标识信息和所述标识信息对应的行为日志，确定所述客户端的身份信息。

8.一种信息溯源装置，其特征在于，包括：

标识信息生成单元，被配置成响应于接收到客户端发送的访问请求，生成与所述客户端相对应的标识信息并发送所述标识信息至所述客户端；

行为日志获取单元，被配置成获取所述标识信息对应的行为日志；

身份信息获取单元，被配置成根据所述标识信息和所述行为日志，确定所述客户端的身份信息；

所述装置还包括：设置模块，用于预先设置信息接收节点，利用所述信息接收节点采集所述标识信息以及溯源信息；

标识信息生成单元，具体用于：

响应于接收到客户端发送的访问请求，所述信息接收节点检测多个域的任意域中是否已存在与所述客户端对应的标识信息；

响应于不存在，所述信息接收节点生成与所述客户端对应的标识信息并发送所述标识信息至所述客户端；

响应于存在，所述信息接收节点发送所述标识信息至所述客户端。

9.一种信息溯源系统，其特征在于，包括服务器和数据分析平台；

所述服务器被配置成响应于预先设置信息接收节点，利用所述信息接收节点采集标识信息以及溯源信息，响应于接收到客户端发送的访问请求，所述信息接收节点检测多个域的任意域中是否已存在与所述客户端对应的标识信息；响应于不存在，所述信息接收节点生成与所述客户端对应的标识信息并发送所述标识信息至所述客户端；响应于存在，所述信息接收节点发送所述标识信息至所述客户端，获取所述标识信息对应的行为日志；以及将所述标识信息和所述行为日志发送至所述数据分析平台；

所述数据分析平台被配置成根据所述标识信息和所述行为日志，确定所述客户端的身份信息。

10.根据权利要求9所述的信息溯源系统，其特征在于，所述服务器还被配置成响应于接收到客户端发送的访问请求，获取所述客户端的溯源信息；以及

所述数据分析平台还被配置成根据所述标识信息、溯源信息和所述行为日志，确定所述客户端的身份信息。

11.根据权利要求10所述的信息溯源系统，其特征在于，所述服务器还包括蜜罐系统；

所述蜜罐系统被配置成响应于所述客户端访问所述蜜罐系统，生成所述标识信息以及获取所述行为日志、所述溯源信息。

12.根据权利要求11所述的信息溯源系统，其特征在于，所述信息溯源系统还包括信息

接收节点,所述信息接收节点被配置成采集所述标识信息以及所述溯源信息。

13.根据权利要求9-12中任一项所述的信息溯源系统,其特征在于,所述服务器还包括真实业务系统;

所述真实业务系统被配置成响应于所述客户端访问所述真实业务系统,生成所述标识信息以及获取所述行为日志。

14.一种电子设备,包括:

一个或多个处理器;

存储装置,其上存储有一个或多个程序;

当所述一个或多个程序被所述一个或多个处理器执行,使得所述一个或多个处理器实现如权利要求1-7中任一项所述的信息溯源方法。

15.一种计算机可读存储介质,其上存储有计算机程序,其中,该程序被处理器执行时实现如权利要求1-7中任一项所述的信息溯源方法。

# 信息溯源方法、装置、系统及存储介质

## 技术领域

[0001] 本申请公开的实施例涉及网络安全技术领域，具体涉及一种信息溯源方法、装置、系统及存储介质。

## 背景技术

[0002] 网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

[0003] 随着科技发展，网络攻击的手段也在不断进化。预先对网络设备进行设置安全防护措施，也通常会被新的恶意攻击技术突破。因此，需要有更加可靠的主动防御手段，确定攻击源头，对恶意攻击者进行事前针对防御、事后追踪取证，即追踪溯源技术。

[0004] 传统的溯源手段主要是追溯IP地址，可以理解为追溯发送攻击数据的主机，但是IP地址很容易被攻击者用代理跳板、僵尸机等方法伪造，这样就需要一级级地逆向追踪，追溯成功的几率和数据可靠性也会在这个过程中大大降低。

[0005] 为了解决上述问题，现有技术中采用客户端溯源手段，即促使攻击者客户端直接向服务端发送标识信息。这样可以规避伪装IP地址这种手段，但是该技术很容易被攻击者发现，不适合大范围使用。并且上述技术会占用服务端较多资源，不便于集成在真实业务系统中。另外，客户端开发技术更迭快，相关溯源手段时效性无法跟上，缺乏稳定的信息关联机制。

## 发明内容

[0006] 有鉴于此，本申请公开的实施例提出了信息溯源方法、装置、系统及存储介质。本申请的信息溯源方法能够在降低资源占用的同时更加隐蔽地实现攻击者身份信息的追踪溯源。

[0007] 第一方面，本申请公开的实施例提供了一种信息溯源方法，该方法包括：响应于接收到客户端发送的访问请求，生成与客户端相对应的标识信息并发送该标识信息至客户端；获取标识信息对应的行为日志；根据该标识信息和该行为日志，确定客户端的身份信息。

[0008] 在优选的实现方式中，该方法还包括：响应于接收到客户端发送的访问请求，获取客户端的溯源信息；以及根据该标识信息和行为日志，确定客户端的身份信息，具体包括：根据该标识信息、溯源信息和行为日志，确定客户端的身份信息。

[0009] 在优选的实现方式中，预先设置蜜罐系统，该方法还包括：响应于客户端访问蜜罐系统，蜜罐系统执行生成标识信息以及获取行为日志、溯源信息的步骤；以及蜜罐系统根据蜜罐系统自身标识生成标识信息，以及将标识信息发送至客户端。

[0010] 在优选的实现方式中，预先设置信息接收节点，该方法还包括：利用信息接收节点采集标识信息以及溯源信息。

[0011] 在优选的实现方式中，响应于接收到客户端发送的访问请求，生成与客户端相对

应的标识信息并发送标识信息至客户端，具体包括：响应于接收到客户端发送的访问请求，信息接收节点检测多个域的任意域中是否已存在于客户端对应的标识信息；响应于不存在，信息接收节点生成与客户端对应的标识信息并发送标识信息至客户端；响应于存在，信息接收节点发送标识信息至客户端。

[0012] 在优选的实现方式中，预先设置真实业务系统，该方法还包括：响应于客户端访问真实业务系统，真实业务系统执行生成标识信息以及获取行为日志的步骤。

[0013] 在优选的实现方式中，真实业务系统执行生成标识信息的步骤，具体包括：真实业务系统根据真实业务系统自身标识生成标识信息，以及将标识信息发送至客户端。

[0014] 在优选的实现方式中，响应于接收到客户端发送的访问请求，生成与客户端相对应的标识信息并发送该标识信息至客户端，具体包括：响应于接收到客户端发送的访问请求，检测客户端是否存在攻击行为；响应于存在攻击行为，生成与客户端对应的标识信息并发送标识信息至客户端；以及根据客户端的攻击行为，对客户端进行分类。

[0015] 在优选的实现方式中，该方法还包括：响应于再次接收到客户端发送的访问请求，查询客户端是否存储有与其相对应的标识信息；响应于客户端未存储有标识信息，生成与客户端相对应的标识信息并发送标识信息至客户端。

[0016] 在优选的实现方式中，根据标识信息和行为日志，确定客户端的身份信息，具体包括：根据多个标识信息和标识信息对应的行为日志，确定客户端的身份信息。

[0017] 第二方面，本申请公开的实施例提供了一种信息溯源装置，该装置包括：标识信息生成单元，被配置成响应于接收到客户端发送的访问请求，生成与客户端相对应的标识信息并发送该标识信息至客户端；行为日志获取单元，被配置成获取该标识信息对应的行为日志；身份信息获取单元，被配置成根据该标识信息和行为日志，确定客户端的身份信息。

[0018] 第三方面，本申请公开的实施例提供了一种信息溯源系统，包括服务器和数据分析平台；服务器被配置成响应于接收到客户端发送的访问请求，生成与客户端相对应的标识信息并发送标识信息至客户端；获取标识信息对应的行为日志；以及将标识信息和行为日志发送至数据分析平台；数据分析平台被配置成根据标识信息和行为日志，确定客户端的身份信息。

[0019] 在优选的实现方式中，服务器还被配置成响应于接收到客户端发送的访问请求，获取客户端的溯源信息；以及数据分析平台还被配置成根据标识信息、溯源信息和行为日志，确定客户端的身份信息。

[0020] 在优选的实现方式中，服务器还包括蜜罐系统；蜜罐系统被配置成响应于客户端访问蜜罐系统，生成标识信息以及获取上述行为日志、溯源信息。

[0021] 在优选的实现方式中，信息溯源系统还包括信息接收节点，该信息接收节点被配置成采集标识信息以及溯源信息。

[0022] 在优选的实现方式中，服务器还包括真实业务系统；真实业务系统被配置成响应于客户端访问真实业务系统，生成标识信息以及获取行为日志。

[0023] 第四方面，本公开的实施例提供了一种电子设备，包括：一个或多个处理器；存储装置，其上存储有一个或多个程序；当一个或多个程序被所述一个或多个处理器执行，使得一个或多个处理器实现如第一方面或第一方面任一实现方式的信息溯源方法。

[0024] 第五方面，本申请公开的实施例提供了一种计算机可读存储介质，其上存储有计

算机程序，其中，该程序被处理器执行时实现如第一方面或第一方面任一实现方式的信息溯源方法。

[0025] 本申请公开的实施例提供的信息溯源的技术方案，若接收到客户端发送的访问请求，则生成与客户端相对应的标识信息并发送该标识信息至客户端，之后，获取该标识信息对应的行为日志，即该客户端的行为日志，然后可以根据该标识信息和行为日志，分析确定客户端的身份信息。在本实施例中，由于在接收到客户端的访问请求时，主动生成标识信息并发送至客户端，客户端会存储该标识信息，这样客户端在进行后续访问或者其他网络行为时，其行为日志会与该标识信息关联，这样通过分析系统中该标识信息对应的行为日志即可追溯出客户端的身份信息，该种主动匹配标识信息的方式主动性强，且容易被集成至各种业务系统中，部署方便，资源占用低，并且隐蔽性高，不易被恶意攻击者发现，进而得到的数据稳定性好，溯源准确；另外，本方案无论恶意客户端技术更迭快慢，都可以将标识信息发送至客户端以与其行为日志关联，因此时效性好。

## 附图说明

[0026] 通过阅读参照以下附图所作的对非限制性实施例所作的详细描述，本公开的其它特征、目的和优点将会变得更明显：

[0027] 图1表示本公开的一个实施例可以应用于其中的示例性系统架构图；

[0028] 图2表示根据本公开的信息溯源方法的一个实施例的流程图；

[0029] 图3表示根据本公开的信息溯源方法的一个实现方式的流程图；

[0030] 图4表示根据本公开的实施例的信息溯源方法的一个应用场景的示意图；

[0031] 图5表示根据本公开的信息溯源方法的又一个实施例的流程图；

[0032] 图6表示根据本公开的信息溯源装置的一个实施例的结构示意图；

[0033] 图7表示根据本公开的信息溯源系统的一个实施例的系统架构图；

[0034] 图8表示根据本公开的信息溯源系统的一个实现方式的系统架构图；

[0035] 图9是适于用来实现本公开的实施例的电子设备的结构示意图。

## 具体实施方式

[0036] 下面结合附图和实施例对本公开作进一步的详细说明。可以理解的是，此处所描述的具体实施例仅仅用于解释相关发明，而非对该发明的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与有关发明相关的部分。

[0037] 需要说明的是，在不冲突的情况下，本公开中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本公开。

[0038] 图1示出了可以应用本公开的信息溯源方法或信息溯源装置的示例性架构图。

[0039] 如图1所示，系统架构100可以包括终端设备101、102、103，网络104和服务器105。网络104用以在终端设备101、102、103和服务器105之间提供通信链路的介质。网络104可以包括各种连接类型，例如有线、无线通信链路或者光纤电缆等等。

[0040] 终端设备101、102、103通过网络104与服务器105交互，以接收或发送消息等。终端设备101、102、103上可以安装有各种通讯客户端应用，例如网页浏览器应用、图像处理类应用、搜索类应用、即时通信工具、邮箱客户端、社交平台软件、文本编辑类应用、阅读类应用

等。

[0041] 终端设备101、102、103可以是硬件，也可以是软件。当终端设备101、102、103为硬件时，可以是具有显示屏并且支持与服务器通信的各种电子设备，包括但不限于智能手机、平板电脑、电子书阅读器、MP3播放器(Moving Picture Experts Group Audio Layer III，动态影像专家压缩标准音频层面3)、MP4(Moving Picture Experts Group Audio Layer IV，动态影像专家压缩标准音频层面4)播放器、膝上型便携计算机和台式计算机等等。当终端设备101、102、103为软件时，可以安装在上述所列举的电子设备中。其可以实现成多个软件或软件模块(例如用来提供分布式服务)，也可以实现成单个软件或软件模块。在此不做具体限定。

[0042] 服务器105可以是提供各种服务的服务器，例如对终端设备101、102、103发送的访问请求进行处理的后台服务器。后台服务器可以生成与终端设备101、102、103分别相对应的标识信息并将该标识信息发送至对应的终端设备。

[0043] 需要说明的是，服务器可以是硬件，也可以是软件。当服务器为硬件时，可以实现成多个服务器组成的分布式服务器集群，也可以实现成单个服务器。当服务器为软件时，可以实现成多个软件或软件模块(例如用来提供分布式服务的软件或软件模块)，也可以实现成单个软件或软件模块。在此不做具体限定。

[0044] 需要说明的是，本公开的实施例所提供的信息溯源方法一般由服务器105执行，相应地，信息溯源装置一般设置于服务器105中。

[0045] 应该理解，图1中的终端设备、网络和服务器的数目仅仅是示意性的。根据实现需要，可以具有任意数目的终端设备、网络和服务器。

[0046] 继续参考图2，示出了根据本公开的信息溯源方法的一个实施例的流程图。该信息溯源方法，应用于服务器，包括以下步骤：

[0047] 步骤201，响应于接收到客户端发送的访问请求，生成与该客户端相对应的标识信息并发送该标识信息至客户端。

[0048] 在本实施例中，信息溯源方法的执行主体(如图1所示的服务器105)若接收到客户端发送的访问请求，则可以主动随机生成与该客户端相对应的标识信息，或者，按照预设的规则生成与该客户端相对应的标识信息，本实施例不以此为限制。

[0049] 标识信息例如可以为字符串，也可以为其他形式表示的信息，本实施例不以此为限制。

[0050] 这里需要说明的是，上述标识信息和客户端是一一对应的关系，即客户端在首次访问服务器时，服务器会生成与该客户端相对应的标识信息，该标识信息是唯一的。

[0051] 在生成与该客户端相对应的标识信息之后，可以将该标识信息发送至客户端，这里的客户端例如可以为上述终端设备101等。这里，服务器可以将该标识信息通过cookie等多种客户端技术存储在客户端，这样当下次该客户端进行其他访问动作或者攻击行为时，其行为日志中会携带有该标识信息，即将该标识信息与客户端的行为进行关联，以便于后续溯源该客户端的身份信息。

[0052] 由于在客户端首次访问服务器时，服务器便可以通过成熟的客户端技术将生成的标识信息存储于客户端，这样在客户端进行其他访问操作时，其行为日志中便会与该标识信息关联，因此，服务器可以将该功能集成于各种业务系统中，部署方便，且相较于现有技

术中需要客户端将标识信息发送至服务器而言，本实施例的技术方案，对于服务器来说资源占用低，且不容易被攻击者客户端发现。

[0053] 步骤202，获取该标识信息对应的行为日志。

[0054] 通过上述步骤201描述可知，当服务器生成标识信息并且使得客户端存储该标识信息之后，客户端再次进行其他网络行为时，其行为日志会与该标识信息关联。这样，服务器可以在整个网络系统中获取该标识信息对应的行为日志，即该客户端对应的行为日志。

[0055] 步骤203，根据该标识信息和行为日志，确定客户端的身份信息。

[0056] 本实施例中，由于在网络系统中，该标识信息存储于客户端，则客户端在进行网络行为时，则其行为日志会与该标识信息关联，因此，在整个系统中一个标识信息可能对应会有多个甚至大量该客户端的行为日志，获取该标识信息和与该标识信息关联的行为日志之后，分析该标识信息和多个行为日志，可以准确追溯客户端的身份信息。

[0057] 作为示例，例如可以解析行为日志中的IP地址、行为发生时间、具体行为等，综合分析确定客户端的主机地址或者设备标识等，本实施例不以此为限制。这里的行为日志的类型可以包括浏览器访问，读写文件或者播放视频等。

[0058] 如图3所示，在较佳的实现方式中，该信息溯源方法可以包括：

[0059] 步骤301，响应于接收到客户端发送的访问请求，生成与该客户端相对应的标识信息并发送该标识信息至客户端。

[0060] 步骤302，获取该标识信息对应的行为日志。

[0061] 上述步骤301和步骤302与前述实施例中的步骤201和步骤202类似，上文针对步骤201和步骤202描述也适用于步骤301和步骤302，此处不再赘述。

[0062] 步骤303，获取客户端的溯源信息。

[0063] 在本实现方式中，在客户端向服务器发送访问请求时，服务器还可以获取客户端的溯源信息。具体地，例如促使客户端向服务器发送自身的设备ID，这样可以避免客户端伪装IP地址。这里的溯源信息包括但不限于客户端的IP地址、攻击行为等。

[0064] 这样，由于在向客户端发送唯一标识信息的同时，还促使客户端向服务器发送溯源信息，因此，本实现方式在避免客户端伪装IP地址的同时，更加精准地从服务器和客户端双向进行信息关联。

[0065] 步骤304，根据该标识信息、溯源信息和行为日志，确定客户端的身份信息。

[0066] 在获取到客户端的溯源信息和行为日志之后，可以结合该标识信息、溯源信息和行为日志，例如解析这些与同一标识信息相对应的溯源信息和行为日志，提取出有用数据，查找客户端的身份信息，例如追溯客户端的设备ID或者网络地址等可以表征其身份的信息。

[0067] 为了提高追溯行为隐蔽性，上述步骤303可以在客户端首次访问服务器时执行，在客户端再次访问时，可以选择性地执行上述步骤303。

[0068] 通过本实现方式，由于在向客户端发送唯一标识信息的同时，还促使客户端向服务器发送溯源信息，因此，本实现方式在避免客户端伪装IP地址的同时，更加精准地从服务器和客户端双向进行信息关联，从而可以使得最终的溯源信息更加准确。

[0069] 在较佳的实现方式中，还可以预先设置蜜罐系统。例如可以设置一些网站为蜜罐系统，若客户端访问该蜜罐系统，则该蜜罐系统可以执行上述步骤301、步骤302和步骤303，

以分别生成标识信息并发送至客户端，获取客户端的行为日志和溯源信息。这样只在蜜罐系统中执行上述步骤303获取客户端的溯源信息，而在服务器的其他服务网站中可以选择性地不执行步骤303，这样可以避免被恶意攻击者发现。

[0070] 在一些较佳的实现方式中，还可以预先设置真实业务系统，真实业务系统相对于安全系统而言，是为用户提供真实服务的系统，例如购票网站、购物网站等。

[0071] 若客户端访问真实业务系统，则真实业务系统可以执行上述步骤201和步骤202，即生成标识信息发送至客户端以及获取与该标识信息对应的行为日志。这样在客户端访问真实业务系统时，只需要生成标识信息以及获取与该标识信息对应的行为日志，一方面可以降低占用服务器的资源，另一方面还可以提高溯源隐蔽性。

[0072] 这里，蜜罐系统和真实业务系统生成标识信息时，可以分别加入自身系统的标识。例如蜜罐系统在生成标识信息时，可以在该标识信息中添加能够表征蜜罐系统的字符，即添加蜜罐系统自身标识；真实业务系统在生成标识信息时，也可以在该标识信息中添加能够表征真实业务系统的字符，即添加真实业务系统自身标识，这样就可以保证各个业务系统在生成标识信息之后，将业务系统与标识信息进行关联，后续进行数据分析时，根据标识信息即可获知是哪个业务系统生成的标识信息，不会混淆，以便于后续进行分析溯源。

[0073] 可以理解，上述“蜜罐系统”和“真实业务系统”只是为了方便描述，在实际应用中，可以将一些网站设置为与上述蜜罐系统类似的功能，将一些网站设置为与上述真实业务系统类似的功能。

[0074] 在一些较佳的实现方式中，还可以预先设置信息接收节点，之后，当客户端访问蜜罐系统和/或真实业务系统时，在客户端被存储标识信息之后，促使客户端将该标识信息和客户端溯源信息发送至信息接收节点，然后再由信息接收节点进行存储，之后根据需要发送至数据处理单元(该数据处理单元例如可以为数据分析平台或者为服务器集群中的某台服务器，本实施例不以此为限制)，这样可以节省网络资源，避免影响蜜罐系统和真实业务系统的自身运行。

[0075] 优选地，若涉及到跨域读取数据，本实现方式可以通过信息接收节点实现，具体地：

[0076] 第一步，响应于接收到客户端发送的访问请求，信息接收节点检测多个域的任意域中是否已存在与客户端对应的标识信息。

[0077] 具体地，可以设置使得多个域之间都能够将客户端的标识信息以及溯源信息发送至信息接收节点，这样信息接收节点便可以获知各个域中该客户端的访问情况。

[0078] 若客户端之前已经访问某一域中的网站，则在该域中的服务器已经生成标识信息并发送至该客户端，当客户端再次访问其他域中的网站时，则信息接收节点先检测在各个域中的任意域中该客户端已经被赋予标识信息，这样可以实现跨域检测。

[0079] 第二步，响应于不存在，信息接收节点生成与该客户端对应的标识信息并发送该标识信息至客户端。

[0080] 具体地，若信息接收节点检测到其他域中不存在该客户端对应的标识信息，则说明该客户端还未存在标识信息，此时信息接收节点可以生成与该客户端对应的标识信息并发送该标识信息至客户端。即新创建标识信息赋予该客户端，使客户端存储该标识信息，以便于将标识信息与客户端的其他网络行为进行关联。

[0081] 第三步，响应于存在，信息接收节点发送该标识信息至客户端。

[0082] 具体地，若信息接收节点检测到其他域中存在该客户端对应的标识信息，则说明该客户端对应的标识信息已经在其访问其他网站时被创建，此时可以将该标识信息发送至客户端，即促使客户端在访问该域中的网站时调用信息接收节点中存储的标识信息。

[0083] 通过本实现方式，可以通过信息接收节点对各网络域中的标识信息存储的特点，实现跨域对客户端进行标识信息关联，进而实现跨域读取数据，使得本公开的信息溯源方法适用范围广，追溯力度大，溯源准确。

[0084] 继续参见图4，图4是根据本公开的实施例的信息溯源方法的应用场景的一个示意图。在图4的应用场景中，服务器401获取客户端402发送的访问请求403。然后，服务器401生成与该客户端402相对应的标识信息404并发送该标识信息404至客户端402。之后，服务器401可以获取该标识信息404对应的行为日志405。然后，结合该标识信息404和行为日志405，追溯出客户端的身份信息406。

[0085] 目前，现有技术之一的客户端溯源技术是通过让客户端将设备ID发送至服务器，该种技术很容易被攻击者客户端识破，不适合大范围使用，并且占用服务端较多资源。而通过本实施例的信息溯源方法，由于在接收到客户端的访问请求时，主动生成标识信息并发送至客户端，客户端会存储该标识信息，这样客户端在进行后续访问或者其他网络行为时，其行为日志会与该标识信息关联，这样通过分析系统中该标识信息对应的行为日志即可追溯出客户端的身份信息，该种主动匹配标识信息的方式主动性强，且容易被集成至各种业务系统中，部署方便，资源占用低，并且隐蔽性高，不易被恶意攻击者发现，进而得到的数据稳定性好，溯源准确；另外，本方案无论恶意客户端技术更迭快慢，都可以将标识信息发送至客户端以与其行为日志关联，因此时效性好。

[0086] 进一步参考图5，其示出了信息溯源方法的又一个实施例的流程图。该信息溯源方法，应用于服务器，包括以下步骤：

[0087] 步骤501，响应于接收到客户端发送的访问请求，检测客户端是否存在攻击行为。

[0088] 在本实施例中，若接收到客户端发送的访问请求，则服务器可以从网络系统中记录的该客户端的网络行为以及该次访问请求的内容来检测识别该客户端是否存在攻击行为。

[0089] 例如客户端之前的网络行为中存在有恶意程序等内容，则说明该客户端极有可能是恶意攻击者。

[0090] 步骤502，响应于存在攻击行为，生成与客户端对应的标识信息并发送该标识信息至客户端。

[0091] 具体地，若检测到该客户端存在攻击行为，这里可以是该客户端之前存在攻击行为，或者是该客户端此次访问请求中存在攻击行为，则说明该客户端为恶意攻击者，服务器可以生成与该客户端对应的标识信息并发送该标识信息至客户端，以使客户端存储该标识信息。这样该客户端的后续行为日志即可以与该标识信息进行关联，便于后续追踪溯源。

[0092] 较佳地，若检测到该客户端之前的网络行为中不存在攻击行为，且此次访问请求中也为正常业务请求，则服务器可以继续执行下述步骤503，但是对于步骤504，服务器可以根据实际需求，在需要追溯该客户端的身份信息时执行，以节省处理器的运算量。

[0093] 步骤503，获取标识信息对应的行为日志；

[0094] 步骤504，根据该标识信息和行为日志，确定客户端的身份信息。

[0095] 在本实施例中，上述步骤503和步骤504分别与前述实施例中的步骤202和步骤203类似，上文针对步骤202和步骤203的描述也适用于步骤503和步骤504，此处不再赘述。

[0096] 从图5中可以看出，与图2对应的实施例相比，本实施例中的信息溯源方法体现了响应于接收到客户端发送的访问请求，检测客户端是否存在攻击行为，响应于存在攻击行为，生成与所述客户端对应的标识信息并发送所述标识信息至所述客户端。由此，本实施例描述的方案，服务器可以在检测到客户端访问时先检测客户端是否存在攻击行为，当其存在攻击行为时再进行追溯客户的身份信息，从而降低处理器的运算量和资源占用，提高处理器的运算效率。

[0097] 在一些较佳的实现方式中，若检测到客户端存在攻击行为，则还可以对客户端进行分类。例如若检测到客户端的攻击行为为恶意写入程序，则可以对该客户端分类为程序篡改攻击者类别，具体分类体现形式可以在生成的上述标识信息中体现，例如用某个字符串表示该类别，这样便于在整个网络系统中，对各类型的攻击者客户端进行分类识别，追溯客户端的身份信息时降低处理器的运算量。

[0098] 在一些较佳的实现方式中，若再次接收到客户端发送的访问请求，服务器还可以先查询客户端是否存储有与其对应的标识信息。若客户端未存储有该标识信息，则生成与客户端相对应的标识信息并发送该标识信息至客户端，这样可以防止遗漏添加标识信息。

[0099] 较佳地，可能会存在一个攻击者产生多个标识信息的情况，例如攻击者使用多个客户端，或者客户端进行重装，或者将客户端强制清空数据，这样会使得多个标识信息实际上对应的是一个攻击者客户端的情况，在本实现方式中，可以结合分析多个标识信息以及每个标识信息对应的行为日志，例如若发现多个标识信息对应的行为日志中存在相同的数据，则很有可能这些标识信息对应的是一个攻击者客户端，或者使用其他算法将多个标识信息关联至同一攻击者客户端，从而形成更加精准的攻击路径图和身份画像，达到准确溯源的目的。

[0100] 进一步参考图6，作为对上述各图所示方法的实现，本公开提供了信息溯源装置600的一个实施例，该装置实施例与图2所示的方法实施例相对应，该装置具体可以应用于各种电子设备中。

[0101] 如图6所示，本实施例提供的信息溯源装置600包括标识信息生成单元601、行为日志获取单元602和身份信息获取单元603。其中，标识信息生成单元601被配置成响应于接收到客户端发送的访问请求，生成与客户端相对应的标识信息并发送标识信息至所述客户端；行为日志获取单元602被配置成获取标识信息对应的行为日志；身份信息获取单元603被配置成根据标识信息和行为日志，确定客户端的身份信息。

[0102] 在本实施例中，信息溯源装置600中：标识信息生成单元601、行为日志获取单元602和身份信息获取单元603的具体处理及其所带来的技术效果可分别参考图2对应实施例中的步骤201、步骤202和步骤203的相关说明，在此不再赘述。

[0103] 本实施例的信息溯源装置600，还可以包括其他一些处理单元或者模块，这些处理单元和模块可以执行上述方法实施例中的方法，在此不在赘述。

[0104] 本公开的上述实施例提供的信息溯源装置，为客户端主动匹配标识信息的方式主动性强，且容易被集成至各种业务系统中，部署方便，资源占用低，并且隐蔽性高，不易被恶

意攻击者发现，进而得到的数据稳定性好，溯源准确；另外，本方案无论恶意客户端技术更迭快慢，都可以将标识信息发送至客户端以与其行为日志关联，因此时效性好。

[0105] 进一步参考图7，作为对上述各图所示方法的实现，本公开提供了信息溯源系统的一个实施例，该信息溯源系统中的各个模块可以与上述方法实施例中的方法相对应。

[0106] 这里，如图7所示，较佳地，该信息溯源系统包括蜜罐系统701、真实业务系统702、信息接收节点703、攻击者704以及数据分析平台705。这里的攻击者704可以理解为客户端。

[0107] 具体地，预先在服务器集群中设置蜜罐系统701。然后，在蜜罐系统701、真实业务系统702中集成能够执行上述方法步骤201的功能模块，在攻击者能够访问到的服务器或者网站中设置信息接收节点703。将信息接收节点703、蜜罐系统701和真实业务系统702中的信息统一关联存储于数据分析平台705。

[0108] 结合图7中的信息交互编号顺序可知，当攻击者704访问蜜罐系统701时，会触发蜜罐系统701中设置的溯源机制，并且蜜罐系统701为该攻击者704创建标识信息。而攻击者704将该标识信息和溯源信息发送至信息接收节点703。蜜罐系统701还可以继续将该标识信息和攻击者704的行为日志发送至数据分析平台705。

[0109] 当同一攻击者访问真实业务系统702时，也会触发真实业务系统702中设置的溯源机制，并且真实业务系统702也可以获取其标识信息并且将该标识信息和行为日志发送至数据分析平台705。当不同攻击者访问真实业务系统702时，真实业务系统702也可以为其创建标识信息。

[0110] 这里，无论攻击者704先访问真实业务系统702还是蜜罐系统701，真实业务系统702和蜜罐系统701均可以对其创建标识信息，并且使其发送溯源信息至信息接收节点703。但是，为了提高溯源隐蔽性，这里可以只在触发蜜罐系统701时使其发送溯源信息至信息接收节点703，而在其触发真实业务系统702时，可以只获取其标识信息和行为日志。且，蜜罐系统701和真实业务系统702可以不需要时刻与数据分析平台705保持通信，而是先将获取的标识信息和行为日志存储于本地，每间隔一段时间发送至数据分析平台705，以节省网络资源。

[0111] 数据分析平台705在接收到上述标识信息、行为日志和溯源信息之后，可以统一综合分析数据库中的这些信息，多维度对攻击者客户端的身份信息进行追溯，例如可以追溯到客户端的设备ID，IP地址等等，本实施例不以此为限制。

[0112] 在一些较佳的实现方式中，考虑到在网络系统中会涉及到跨域读取数据的问题，如图8所示，本实现方式提供了在跨域时的信息交互示意图。

[0113] 当攻击者704访问蜜罐系统701时，会触发蜜罐系统701中的溯源机制，促使攻击者客户端向信息接收节点703调用标识信息，这里，信息接收节点703可以先检测多个域的任意域中是否已存在与该客户端对应的标识信息；若不存在，则信息接收节点703生成与客户端对应的标识信息并发送标识信息至客户端；若存在，则信息接收节点发送已经存在的该标识信息至客户端。具体的实现方式可以参考上述方法实施例中的具体描述，此处不再赘述。

[0114] 当攻击者704访问真实业务系统702时，其原理同上述访问蜜罐系统701时类似。

[0115] 下面参考图9，下面参考图9，其示出了适于用来实现本公开的实施例的电子设备(例如图1中的服务器)的结构示意图。图9示出的服务器仅仅是一个示例，不应对本公开的

实施例的功能和使用范围带来任何限制。

[0116] 如图9所示，该电子设备可以包括处理装置(例如中央处理器、图形处理器等)901，其可以根据存储在只读存储器(ROM)902中的程序或者从存储装置908加载到随机访问存储器(RAM)903中的程序而执行各种适当的动作和处理。在RAM 903中，还存储有电子设备操作所需的各种程序和数据。处理装置901、ROM 902以及RAM 903通过总线904彼此相连。输入/输出(I/O)接口905也连接至总线904。

[0117] 通常，以下装置可以连接至I/O接口905：包括例如触摸屏、触摸板、键盘、鼠标、摄像头、麦克风、加速度计、陀螺仪等的输入装置906；包括例如液晶显示器(LCD，Liquid Crystal Display)、扬声器、振动器等的输出装置907；包括例如磁带、硬盘等的存储装置908；以及通信装置909。通信装置909可以允许电子设备与其他设备进行无线或有线通信以交换数据。虽然图9示出了具有各种装置的电子设备，但是应理解的是，并不要求实施或具备所有示出的装置。可以替代地实施或具备更多或更少的装置。图9中示出的每个方框可以代表一个装置，也可以根据需要代表多个装置。

[0118] 特别地，根据本公开的实施例，上文参考流程图描述的过程可以被实现为计算机软件程序。例如，本公开的实施例包括一种计算机程序产品，其包括承载在计算机可读介质上的计算机程序，该计算机程序包含用于执行流程图所示的方法的程序代码。在这样的实施例中，该计算机程序可以通过通信装置909从网络上被下载和安装，或者从存储装置908被安装，或者从ROM 902被安装。在该计算机程序被处理装置901执行时，执行本公开的实施例的方法中限定的上述功能。

[0119] 需要说明的是，本公开的实施例所述的计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质或者是上述两者的任意组合。计算机可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。计算机可读存储介质的更具体的例子可以包括但不限于：具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机访问存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。

[0120] 以上描述仅为本公开的较佳实施例以及对所运用技术原理的说明。本领域技术人员应当理解，本公开的实施例中所涉及的发明范围，并不限于上述技术特征的特定组合而成的技术方案，同时也应涵盖在不脱离上述发明构思的情况下，由上述技术特征或其等同特征进行任意组合而形成的其它技术方案。例如上述特征与本公开的实施例中公开的(但不限于)具有类似功能的技术特征进行互相替换而形成的技术方案。

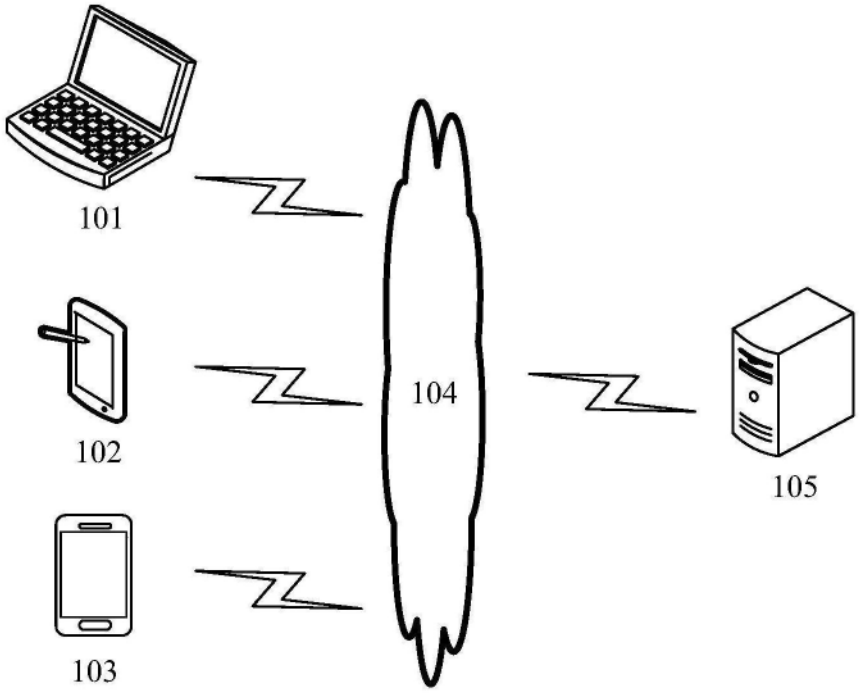

101
102
103
104
105

图1

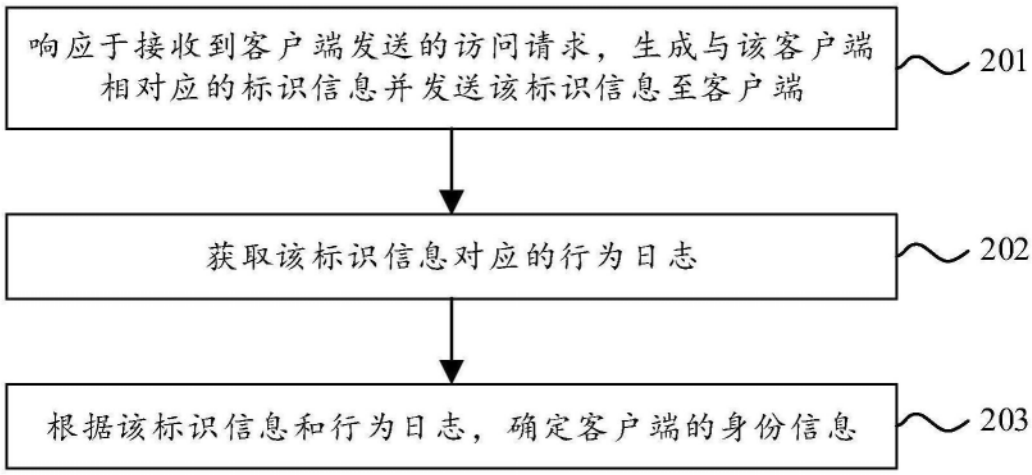

响应于接收到客户端发送的访问请求，生成与该客户端相对应的标识信息并发送该标识信息至客户端
201
获取该标识信息对应的行为日志
202
根据该标识信息和行为日志，确定客户端的身份信息
203

图2

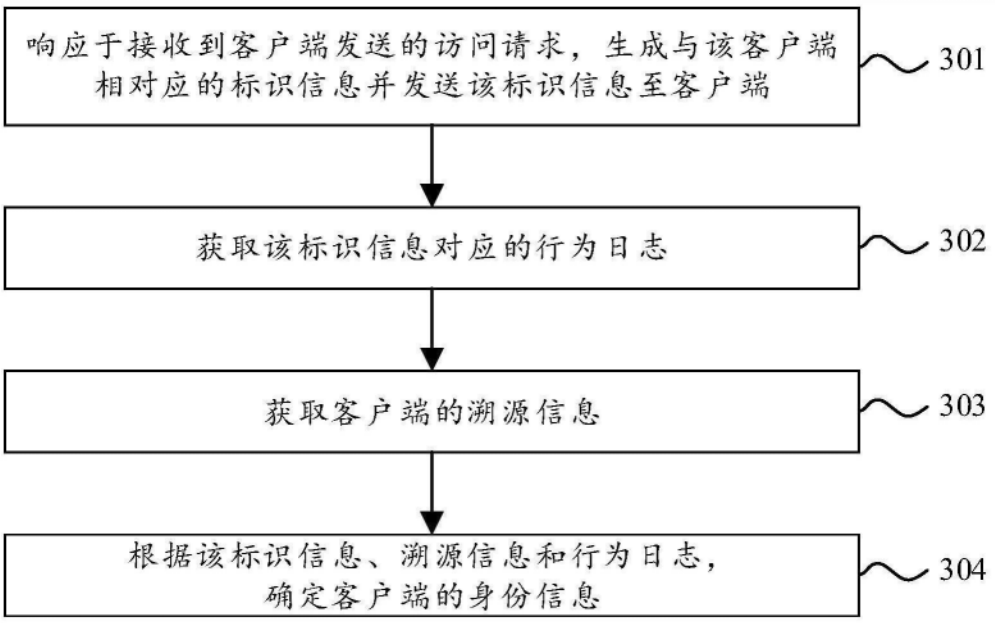

响应于接收到客户端发送的访问请求，生成与该客户端相对应的标识信息并发送该标识信息至客户端
301
获取该标识信息对应的行为日志
302
获取客户端的溯源信息
303
根据该标识信息、溯源信息和行为日志，确定客户端的身份信息
304

图3

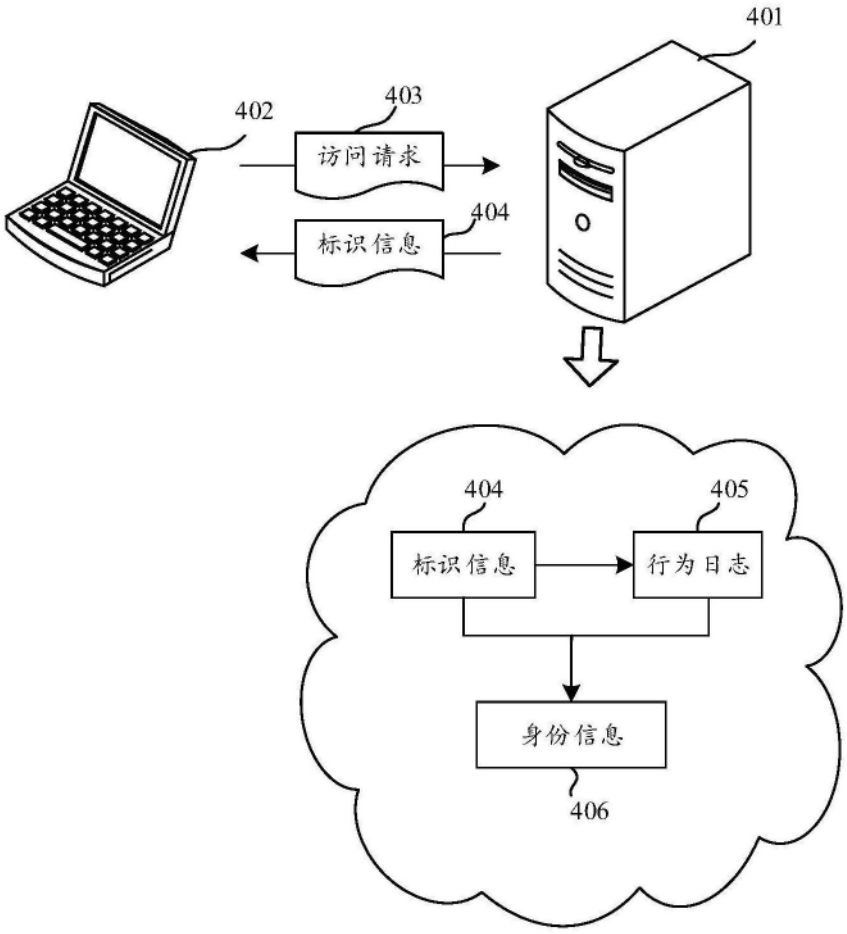

401
402
403
访问请求
404
标识信息
404
405
标识信息
行为日志
身份信息
406

图4

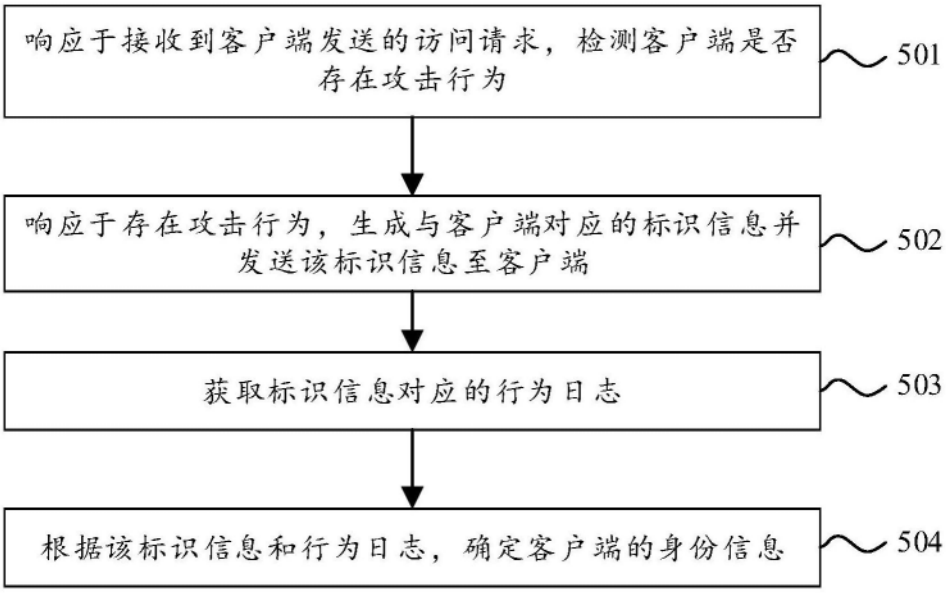

响应于接收到客户端发送的访问请求，检测客户端是否存在攻击行为
501
响应于存在攻击行为，生成与客户端对应的标识信息并发送该标识信息至客户端
502
获取标识信息对应的行为日志
503
根据该标识信息和行为日志，确定客户端的身份信息
504

图5

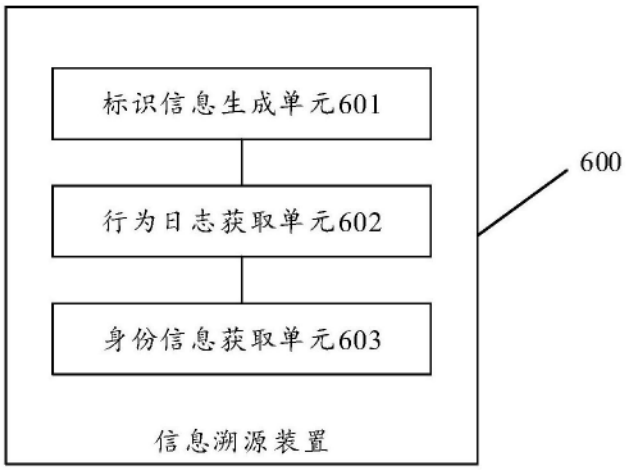

标识信息生成单元601
行为日志获取单元602
身份信息获取单元603
信息溯源装置
600

图6

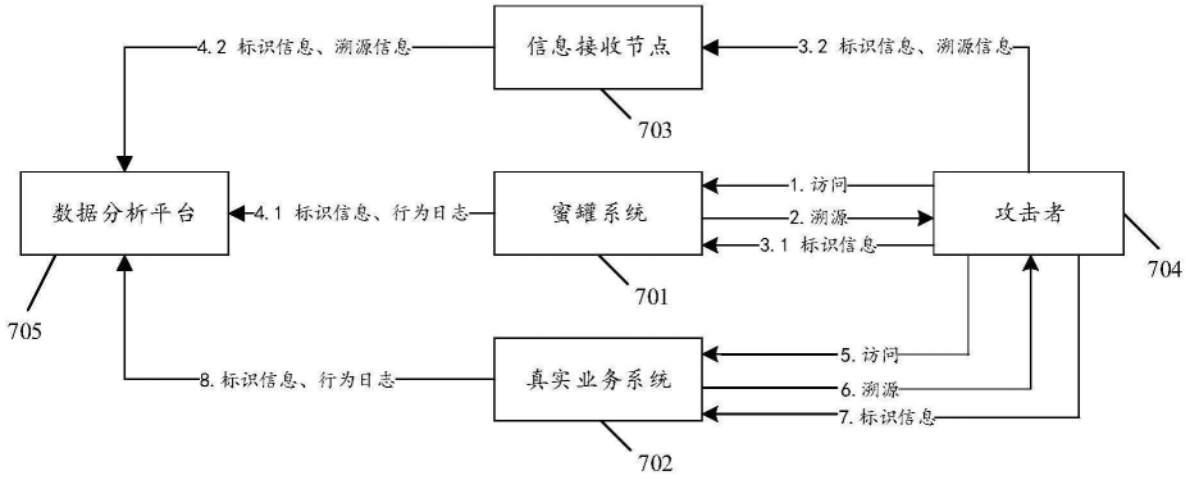

信息接收节点
703
4.2 标识信息、溯源信息
3.2 标识信息、溯源信息
数据分析平台
4.1 标识信息、行为日志
蜜罐系统
701
1. 访问
2. 溯源
3.1 标识信息
攻击者
704
705
8. 标识信息、行为日志
真实业务系统
702
5. 访问
6. 溯源
7. 标识信息

图7

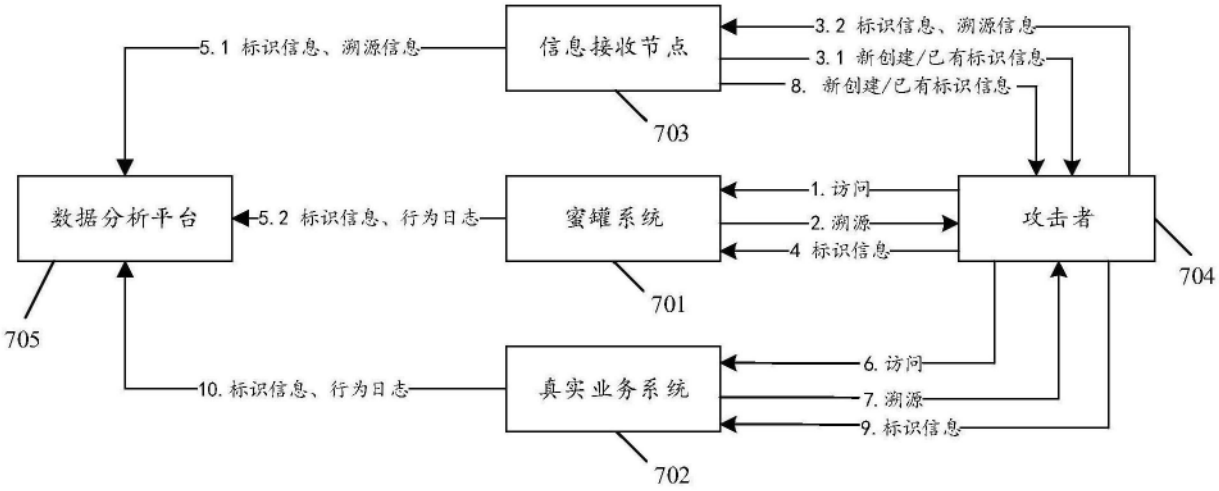

信息接收节点
703
5.1 标识信息、溯源信息
3.2 标识信息、溯源信息
3.1 新创建/已有标识信息
8. 新创建/已有标识信息
数据分析平台
5.2 标识信息、行为日志
蜜罐系统
701
1. 访问
2. 溯源
4 标识信息
攻击者
704
705
10. 标识信息、行为日志
真实业务系统
702
6. 访问
7. 溯源
9. 标识信息

图8

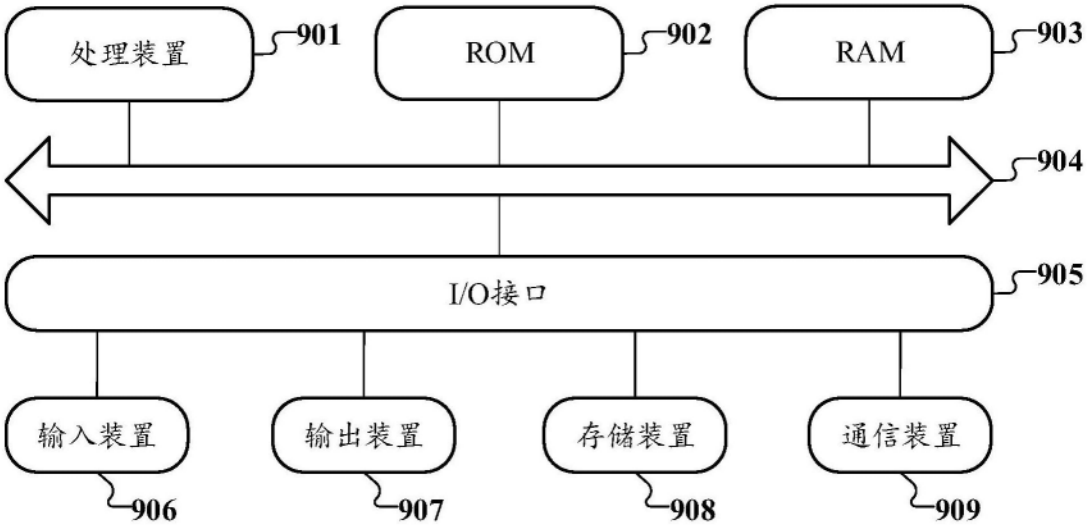

处理装置
901
ROM
902
RAM
903
904
I/O接口
905
输入装置
906
输出装置
907
存储装置
908
通信装置
909

图9