(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 103714456 B
(45)授权公告日 2015.08.19

(21)申请号 201410014450.6
(22)申请日 2014.01.06
(73)专利权人 同济大学
地址 200092 上海市杨浦区四平路1239号
(72)发明人 蒋昌俊 陈闵中 闫春钢 丁志军 于汪洋 钟珺竹
(74)专利代理机构 上海天协和诚知识产权代理事务所 31216
代理人 叶凤
(51)Int.Cl.
H04L 29/06(2006.01)
G06Q 20/38(2012.01)

(56)对比文件
CN 1900963 A,2007.01.24, 全文.
CN 101652755 A,2010.02.17, 全文.
CN 103489101 A,2014.01.01, 全文.
JP 2008-234520 A,2008.10.02, 全文.

审查员 刘莹莹

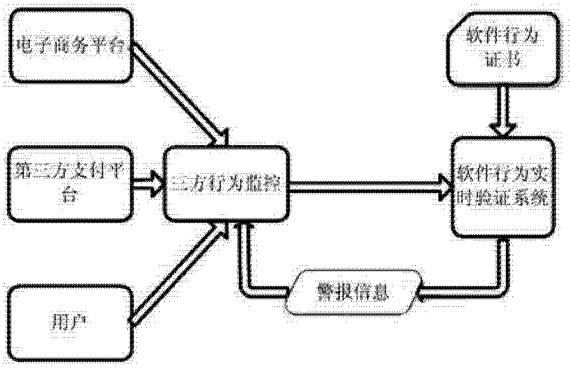
权利要求书1页 说明书3页 附图5页

(54)发明名称

软件行为监控验证系统

(57)摘要

本发明涉及一种软件行为监控验证系统，由软件行为证书、三方软件行为监控器、软件行为实时验证系统三个部分组成；软件行为证书是根据用户，电子商务网站，第三方支付平台在正确交易流程下的三方通信数据包；三方软件行为监控器，是安装于电子商务网站、第三方支付平台、用户客户端上的数据包监控器；软件行为实时验证系统在接收三方监控器分别提交的交易交互信息数据包后，提取并整合其中的关键序列与信息，并根据全球唯一订单号，将用户行为交互序列与软件行为模型进行实时对比，一旦发生乱序，假冒身份等非法行为则进行警报并关闭交易。本发明利用三方交互url等关键参数，刻画合法正常三方交易交互流程，提出了软件行为证书。



CN 103714456 B

1.一种软件行为监控验证系统，其特征在于，由软件行为证书、三方软件行为监控器、软件行为实时验证系统三个部分组成；

所述软件行为证书是根据用户，电子商务网站，第三方支付平台在正确交易流程下的三方通信数据包，从而由专业人员人为刻画三方正常合法交互行为，形成软件行为证书；所述软件行为证书是电子商务网站、第三方支付平台、用户客户端三者，包括两两之间各自形成的交互模式，形成对应的软件行为模型；

所述三方软件行为监控器，是安装于电子商务网站、第三方支付平台、用户客户端上的数据包监控器，用来实时监控在一次完整交易中参与交易的三方之间相互传递的数据包，并且进行数据包中的必要参数信息的提取和整合，便于将关键信息发送给软件行为实时验证系统；所述监控器以 jpcap 为技术基础，主要捕获 http 协议数据包，并提取数据包中的 URL 地址及参数信息，以及交易三方中电商编号和第三方支付平台编号；随后与软件行为实时验证系统建立 socket 连接，将关键信息以 tcp 数据包的形式发送给软件行为实时验证系统；

所述软件行为实时验证系统在接收三方监控器分别提交的交易交互信息数据包后，提取并整合其中的关键序列与信息，并根据全球唯一订单号，将用户行为交互序列与软件行为模型进行实时对比，一旦发生乱序，假冒身份非法行为则进行警报并关闭交易。

2.根据权利要求 1 所述的软件行为监控验证系统，其特征在于，所述软件行为证书中刻画的软件行为有着一定的行为逻辑，体现在：

1) 软件行为证书中每一个 transition_node 为一个行为结点，三方中任一方所捕捉到的数据包分为两大类：接收的消息，发送的消息，分别对应 transition_node 中的 input，output，两者有着必要的逻辑顺序，接收消息必须先于发送消息；将捕获到的行为序列与相对应的 transition_node 相对比，一旦违反上述逻辑顺序则进行警报；

2) 与此同时，软件行为实时验证系统还将接收或者发送消息的当前主体与证书行为结点 transition_node 中属性 attri 所记录的主体名称进行对比，如不相符则意味着非法用户身份冒充攻击，立即警报；

3)place_node 则刻画了行为结点与行为结点之间的逻辑顺序，行为结点 transition_node 也必须按照一定的交易顺序排列，一旦发生跳跃，乱序则意味着合法正常交易流程被打破，出现了违规操作，立即警报。

软件行为监控验证系统

技术领域

[0001] 本发明涉及电子商务网络交易安全监控技术领域。

背景技术

[0002] 随着 Internet 的发展， 电子商务（E—Commerce）已经逐渐成为人们进行商务活动的新模式，也越来越成为国际贸易中重要的经营模式。它以计算机技术、通信技术与网络技术为基础，利用电子数据交换、电子邮件、电子支付等方式实现了整个商务活动的电子化、数字化和网络化。电子交易平台的出现，使整个销售、交易和确认的程序已被网上交易所取代。由从前第一代的银行交易系统 Electronic Brokerage System(EBS)，发展至银行自行研发的单一交易平台，到今天由第三方提供的多主体交易平台，以及由市场推动的应用程序接口（API），都显示出电子交易迅猛发展的势头，但它的发展还面临着许多机遇和调整。

[0003] 近年来，电子商务模式主要由 B2C, B2B 和 C2C 构成，但这些模式也都普遍采用第三方支付的模式，用户、电子商务网站、第三方支付平台是目前电子交易过程中的三个主要主体。上述三方通过签名，认证，加密等技术相互信任，互相调用接口进行通信，从而协作完成整个网上交易过程。然而由于当今软件开发技术的不够完善，在用户客户端软件，电子商务网站，甚至是第三方支付平台都可能存在着一定的通信接口漏洞和逻辑错误等。

[0004] 本发明面向的情况是合法注册的恶意用户往往可以利用这些漏洞从事非法行为，为自己谋取非法利益。并且由于这种漏洞的隐藏性，多样性和难以防范性、用户行为的多变性、以及网络平台的分布式与松耦合性，这三者因素综合，导致传统的安全方法无法保证现今电子网络交易安全。

发明内容

[0005] 本发明的目的在于克服现有技术的不足，公开了一种软件行为监控验证系统，提出用户、电子商务平台、第三方支付平台三方相互协作的安全保证模式，交易流程全程监控，实时警报。

[0006] 本发明给出的技术方案为：

[0007] 一种软件行为监控验证系统，其特征在于，由软件行为证书、三方软件行为监控器、软件行为实时验证系统三个部分组成。

[0008] 所述软件行为证书是根据用户，电子商务网站，第三方支付平台在正确交易流程下的三方通信数据包，从而由专业人员人为刻画三方正常合法交互行为，形成软件行为证书。所述软件行为证书是电子商务网站、第三方支付平台、用户客户端三者，包括两两之间各自形成的交互模式，形成对应的软件行为模型。

[0009] 所述三方软件行为监控器，是安装于电子商务网站、第三方支付平台、用户客户端上的数据包监控器，用来实时监控在一次完整交易中参与交易的三方之间相互传递的数据包，并且进行数据包中的必要参数信息（URL 地址，参数等）的提取和整合，便于将关键信息

发送给软件行为实时验证系统。所述监控器以 jpcap 为技术基础，主要捕获 http 协议数据包，并提取数据包中的 URL 地址及参数信息，以及交易三方中电商编号和第三方支付平台编号。随后与软件行为实时验证系统建立 socket 连接，将关键信息以 tcp 数据包的形式发送给软件行为实时验证系统。

[0010] 所述软件行为实时验证系统在接收三方监控器分别提交的交易交互信息数据包后，提取并整合其中的关键序列与信息，并根据全球唯一订单号，将用户行为交互序列与软件行为模型进行实时对比，一旦发生乱序，假冒身份等非法行为则进行警报并关闭交易。

[0011] 所述软件行为证书中刻画的软件行为有着一定的行为逻辑，体现在：

[0012] 1）软件行为证书中每一个 transition_node 为一个行为结点，三方中任一方所捕捉到的数据包分为两大类：接收的消息，发送的消息，分别对应 transition_node 中的 input，output，两者有着必要的逻辑顺序，接收消息必须先于发送消息；将捕获的到行为序列与相对应的 transition_node 相对比，一旦违反上述逻辑顺序则进行警报；

[0013] 2）与此同时，软件行为实时验证系统还将接收或者发送消息的当前主体与证书行为结点（transition_node）中属性 attri 所记录的主体名称进行对比，如不相符则意味着非法用户身份冒充攻击，立即警报；

[0014] 3）place_node 则刻画了行为结点与行为结点之间的逻辑顺序，行为结点（transition_node）也必须按照一定的交易顺序排列，一旦发生跳跃，乱序则意味着合法正常交易流程被打破，出现了违规操作，立即警报。

[0015] 本发明的创新点及其有益效果：利用三方交互 url 等关键参数，刻画合法正常三方交易交互流程，提出了软件行为证书。软件行为证书是根据用户，电子商务网站，第三方支付平台在正确交易流程下的三方通信数据包，从而由专业人员人为刻画三方正常合法交互行为，形成软件行为证书。本发明提出用户，电子商务平台，第三方支付平台三方相互协作的安全保证模式，交易流程全程监控，实时警报。

附图说明

[0016] 图 1 是软件行为监控验证整体架构图。

[0017] 图 2 三方软件行为监控器流程图。

[0018] 图 3 软件行为实时验证系统流程图。

[0019] 图 4 软件行为证书格式（place_node）。

[0020] 图 5 软件行为证书格式（transition_node）。

具体实施方式

[0021] 整个软件行为监控验证系统的架构如图 1 所示。

[0022] 整个软件行为监控验证系统将真正合法用户的行为固化下来形成软件行为证书。然后主要根据全球唯一订单号，将交易过程中的三方交互行为序列与软件行为证书进行实时对比，单步验证，一旦任何一方发生消息乱序或者假冒身份等非法行为则进行警报或采取一定的措施。

[0023] 三方软件行为监控器：在电子商务网站、第三方支付平台以及用户客户端安装数据包监控器，用来实时监控在一次完整交易中参与交易的三方之间相互传递的数据包，并

且进行数据包中的必要参数信息的提取和整合，便于将关键信息发送给软件行为实时验证系统。所述监控器以 jpcap 为技术基础，主要捕获 http 协议数据包，并提取数据包中的 URL 地址及参数信息，以及交易三方中电商编号和第三方支付平台编号。随后与软件行为实时验证系统建立 socket 连接，将关键信息以 tcp 数据包的形式发送给软件行为实时验证系统。三方软件行为监控流程图如图 2 所示：

[0024] 软件行为实时验证系统：在与三方软件行为监控器建立 socket 连接之后，接收三方软件行为监控器发送过来的 tcp 数据包，提取并整合其中的关键序列与信息。然后根据全球唯一订单号，将用户行为交互序列与软件行为模型进行实时验证，一旦发生乱序，假冒身份等非法行为则进行警报并关闭交易。软件行为实时验证系统流程图如图 3 所示：

[0025] 电子商务网站与第三方支付平台，以及用户客户端三者，包括两两之间各自的交互模式所形成的软件行为证书。软件行为证书由专业人员手动构建，并以 XML 文件格式存储在服务器中。

[0026] 软件行为证书格式如图 4, 图 5 所示：

[0027] input 为三方(用户，电子商务网站，第三方支付平台)中任一方接收到的关键参数(url 等)。output 为当前方发送的关键参数。这些交互信息代表了软件行为序列。

[0028] 软件行为证书中刻画的软件行为有着一定的行为逻辑。这种逻辑体现了三方交互顺序，前提条件等。软件行为证书中每一个 transition_node 为一个行为结点。三方中任一方所捕捉到的数据包分为两大类：接收的消息，发送的消息。分别对应 transition_node 中的 input，output。而两者也有着必要的逻辑顺序，接收消息必须先于发送消息。我们将捕获的到行为序列与相对应的 transition_node 相对比，一旦违反上述逻辑顺序则进行警报。与此同时，软件行为实时验证系统还将接收或者发送消息的当前主体与证书行为结点(transition_node)中属性 attri 所记录的主体名称进行对比，如不相符则意味着非法用户身份冒充攻击，立即警报。place_node 则刻画了行为结点与行为结点之间的逻辑顺序。也就是说行为结点(transition_node)也必须按照一定的交易顺序排列，一旦发生跳跃，乱序则意味着合法正常交易流程被打破，出现了违规操作，立即警报。

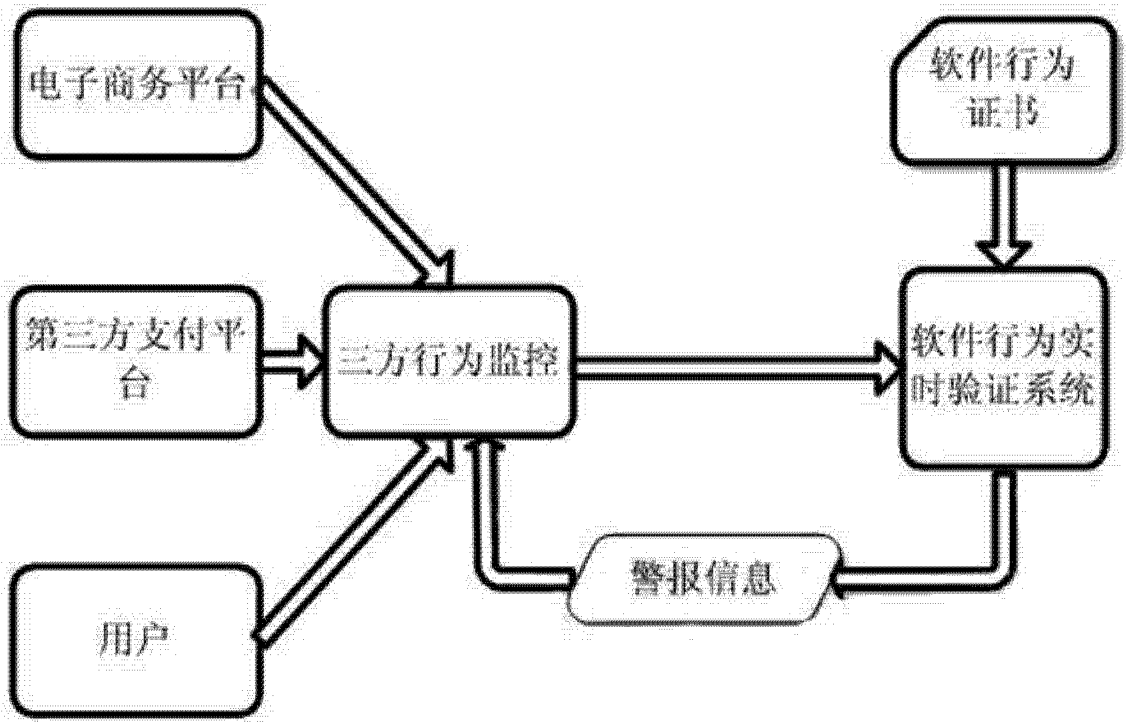


图 1

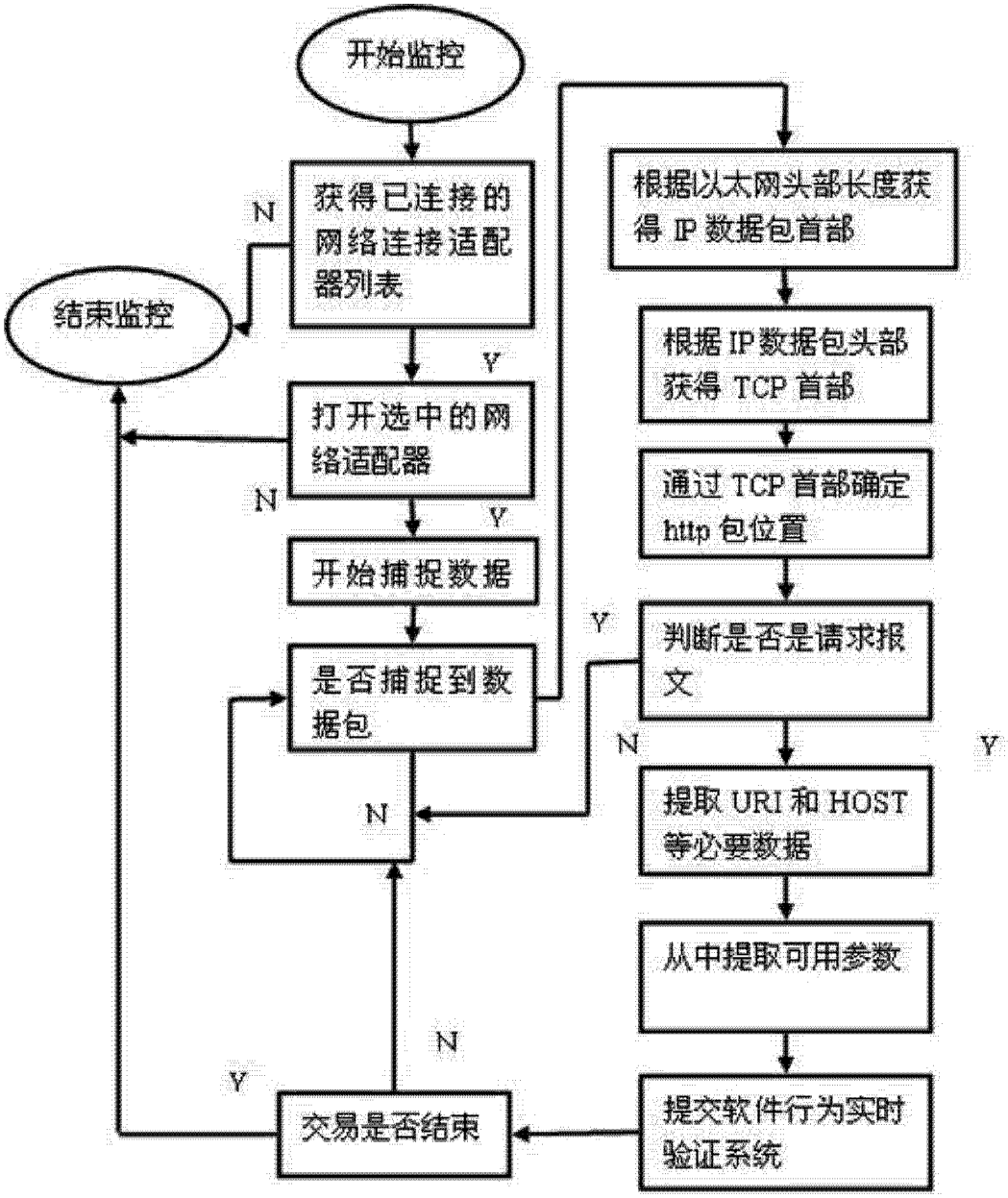

开始监控
获得已连接的网络连接适配器列表
N
结束监控
Y
打开选中的网络适配器
N
Y
开始捕捉数据
是否捕捉到数据包
N
Y
根据以太网头部长度获得 IP 数据包首部
根据 IP 数据包头部获得 TCP 首部
通过 TCP 首部确定 http 包位置
判断是否是请求报文
Y
N
Y
提取 URI 和 HOST 等必要数据
从中提取可用参数
提交软件行为实时验证系统
N
Y
交易是否结束

图 2

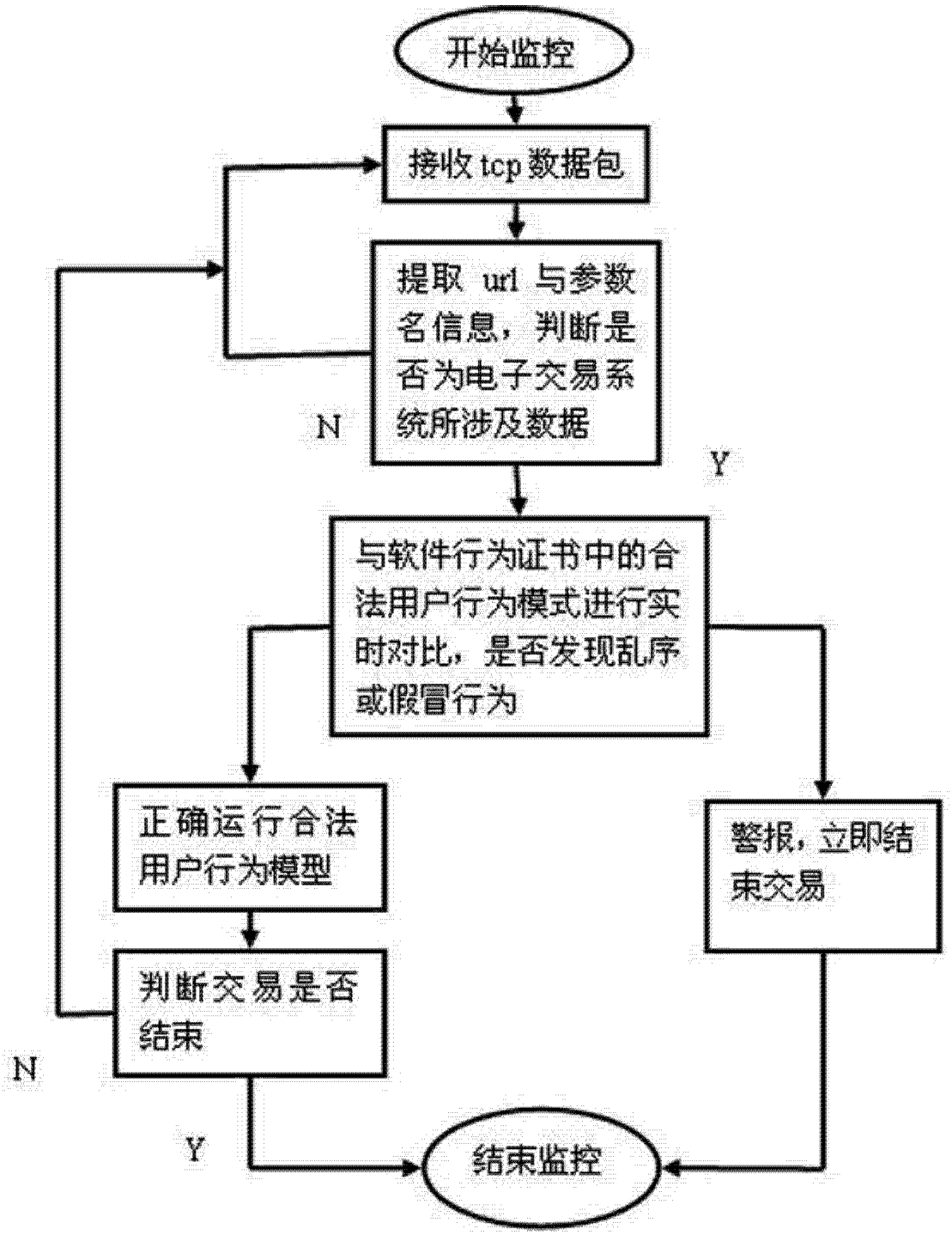

开始监控
接收 tcp 数据包
提取 url 与参数名信息，判断是否为电子交易系统所涉及数据
N
Y
与软件行为证书中的合法用户行为模式进行实时对比，是否发现乱序或假冒行为
正确运行合法用户行为模型
警报，立即结束交易
判断交易是否结束
N
Y
结束监控

图 3

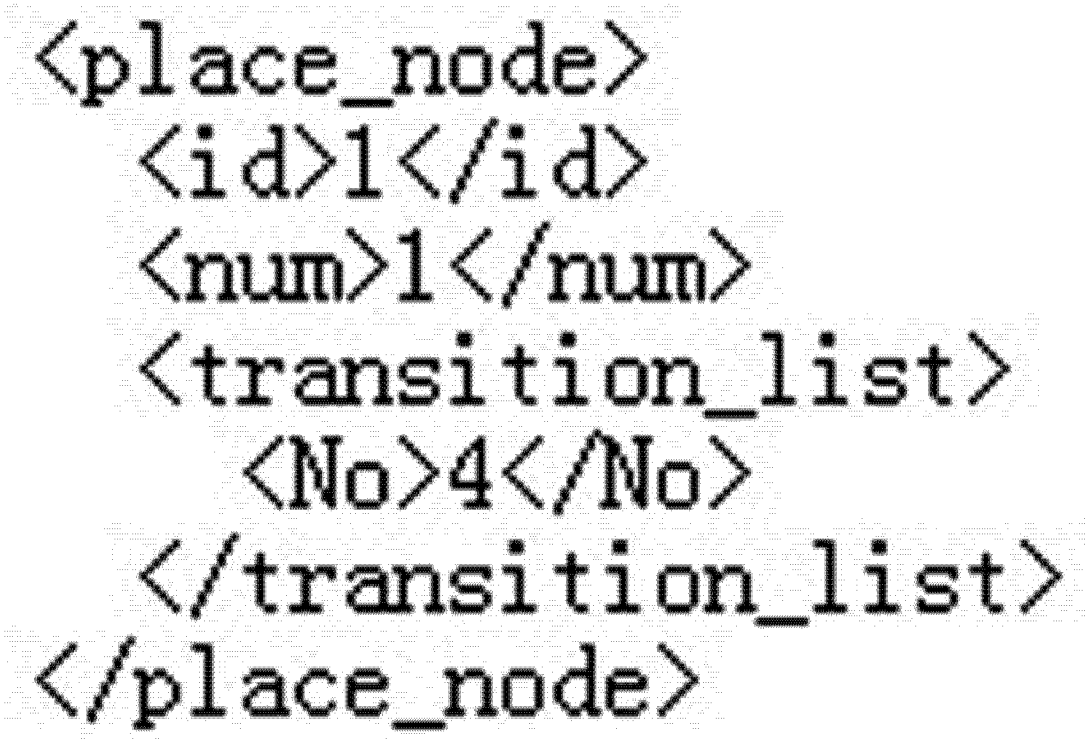

<place_node>
<id>1</id>
<num>1</num>
<transition_list>
<No>4</No>
</transition_list>
</place_node>

图 4

```
<transition_node>
  <id>5</id>
  <name>HandleIPN</name>
  <attri>merchant</attri>
  <outplace>
    <No>11</No>
    <No>12</No>
  </outplace>
  <inplace>
    <No>6</No>
    <No>8</No>
  </inplace>
  <input>
    <string>orderID</string>
    <string>gross</string>
    <string>status</string>
    <string>hidden</string>
    <string>merchantID</string>
    <string>caasID</string>
    <string>uniqueID</string>
  </input>
  <output>
    <string>http://10.60.149.180/Caas/servlet/Get_down?</string>
    <string>junzhu</string>
    <string>orderID</string>
    <string>merchantID</string>
    <string>caasID</string>
    <string>uniqueID</string>
  </output>
</transition_node>
```

图 5