(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 107251513 B
(45)授权公告日 2020.06.09

(21)申请号 201580074497.4

(22)申请日 2015.11.24

(65)同一申请的已公布的文献号
申请公布号 CN 107251513 A

(43)申请公布日 2017.10.13

(30)优先权数据
62/083,985 2014.11.25 US
62/147,040 2015.04.14 US

(85)PCT国际申请进入国家阶段日
2017.07.25

(86)PCT国际申请的申请数据
PCT/IL2015/051139 2015.11.24

(87)PCT国际申请的公布数据
WO2016/084076 EN 2016.06.02

(73)专利权人 恩西洛有限公司
地址 以色列荷兹利亚市

(72)发明人 罗伊·喀特莫尔 汤默尔·比东尤的·雅沃 伊多·凯乐荪

(74)专利代理机构 上海翼胜专利商标事务所（普通合伙）31218
代理人 翟羽

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

(56)对比文件
US 2012303731 A1,2012.11.29,
US 2014082739 A1,2014.03.20,
US 2012030731 A1,2012.02.02,
CN 103716284 A,2014.04.09,
CN 102360408 A,2012.02.22,
CN 101206467 A,2008.06.25,
CN 101112063 A,2008.01.23,

审查员 曾康玲

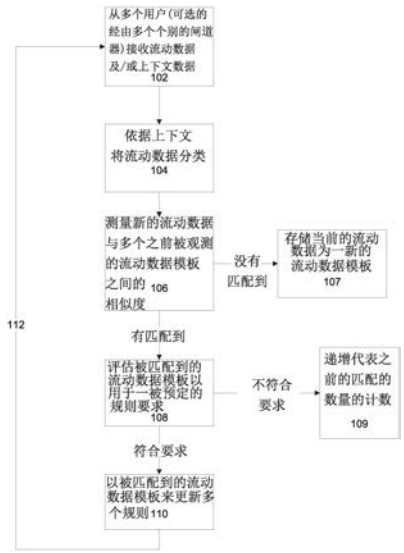
权利要求书4页 说明书20页 附图5页

(54)发明名称

用于恶意代码检测的准确保证的系统及方法

(57)摘要

本发明提供一种方法，用于认证由一被允许的代码建立一网络连线的一企图，所述方法包含：提供具有多个之前被观测的多个堆栈跟踪模板的一数据集，其中所述多个堆栈跟踪模板的每一个代表在多个堆栈跟踪中普遍存在的一堆栈跟踪模式，其中所述多个堆栈跟踪是通过监控多个用户的多个堆栈而记录，其中所述多个用户是在一连线建立过程中执行一被允许的代码，其中所述连线建立过程是用于建立与所述被允许的代码相关的多个网络连线；接收一新的堆栈跟踪，其中所述新的堆栈跟踪是在用于一新的网络连线的一新的连线建立过程中被一新的用户记录；测量所述新的堆栈跟踪与所述多个堆栈跟踪模板之间的一相似度，以识别与一堆栈跟踪模板的一匹配；评估所述被匹配到的堆栈跟踪模板，以用于一被预定的规则要求；及以所述被匹配到的堆栈跟踪模板来更新一规则集数据库，以认证与多个堆栈模板相关联的多个新的网络连线建立，其中所述多个堆栈模板与所述被匹配到的堆栈跟踪模板相匹配。



CN 107251513 B

1.一种用于认证由一被允许的代码建立一网络连线的一企图的方法,其特征在于:所述方法包含步骤:

提供具有多个之前被观测的多个堆栈跟踪模板的一数据集,其中所述多个堆栈跟踪模板的每一个代表在多个堆栈跟踪中普遍存在的一堆栈跟踪模式,其中所述多个堆栈跟踪是通过监控多个用户的多个堆栈而记录,其中所述多个用户是在一连线建立过程中执行一被允许的代码,其中所述连线建立过程是用于建立与所述被允许的代码相关的多个网络连线;

接收一新的堆栈跟踪,其中所述新的堆栈跟踪是在用于一新的网络连线的一新的连线建立过程中被一新的用户记录;

测量所述新的堆栈跟踪与所述多个堆栈跟踪模板之间的一相似度,以识别一被匹配到的堆栈跟踪模板;

评估所述被匹配到的堆栈跟踪模板,以用于一被预定的规则要求;及

以所述被匹配到的堆栈跟踪模板来更新一规则集数据库,以认证与多个堆栈模板相关联的多个新的网络连线建立,其中所述多个堆栈模板与所述被匹配到的堆栈跟踪模板相匹配;

其中评估所述被匹配到的堆栈跟踪模板的步骤包含:

递增一计数器的一值,其中所述计数器指示从多个不同的用户而来的多个之前堆栈跟踪模板匹配;及

评估所述值是否违反多个匹配的所述被预定的规则要求。

2.如权利要求1所述的方法,其特征在于:所述多个堆栈跟踪模板被指定为代表所述被允许的代码的一可疑恶意行为。

3.如权利要求1所述的方法,其特征在于:所述多个堆栈跟踪模板及所述新的堆栈跟踪包括被以与所述被允许的代码的所述堆栈跟踪相关联的方式收集的一上下文数据,及所述相似度是依据所述上下文数据而被测量。

4.如权利要求3所述的方法,其特征在于:所述上下文数据包括一事件识别码及/或一主机名称。

5.如权利要求3所述的方法,其特征在于:所述上下文数据包括选自由下述组成的群组中的至少一成员:在个别的用户处运行的一相似操作系统、一相似被允许的应用程序、多个不同被允许的应用程序的一相似堆栈跟踪数据,及建立所述网络连线的多个相似协议。

6.如权利要求1所述的方法,其特征在于:所述方法还包含:基于所述匹配的不存在,将所述新的堆栈跟踪加入所述数据集成为一新的堆栈跟踪模板。

7.如权利要求1所述的方法,其特征在于:所述多个不同的用户为一相同被指定的群组的一部分。

8.如权利要求1所述的方法,其特征在于:当所述被匹配到的堆栈跟踪模板及所述新的堆栈跟踪与多个不同的用户相关联时,评估所述被匹配到的堆栈跟踪模板的步骤即被进行,以用于所述被预定的规则要求。

9.如权利要求1所述的方法,其特征在于:所述方法还包含:

分析所述新的堆栈跟踪以指定所述网络连线为怀疑与一恶意代码相关;及

所述方法还包含:

重指定与所述恶意代码相关的所述怀疑为与所述被允许的代码相关。

10.如权利要求9所述的方法，其特征在于：与所述恶意代码相关的所述怀疑是由一新的被允许的代码所引起，其中所述新的被允许的代码被安装于显示一像恶意的行为的所述新的用户上。

11.如权利要求9所述的方法，其特征在于：所述被允许的代码代表由不正确地引起怀疑与所述恶意代码相关的所述识别而来的一假阳性识别。

12.如权利要求9所述的方法，其特征在于：所述堆栈跟踪被与至少一堆栈跟踪模板匹配，其中所述堆栈跟踪与一被认证通过的新的网络连线相关联，及所述至少一堆栈跟踪模板与建立用于一恶意通信的所述网络连线的一企图相关联。

13.如权利要求1所述的方法，其特征在于：所述新的堆栈跟踪及所述多个堆栈跟踪模板还包含一流动数据，包括选自由下述组成的群组中的至少一成员：多个程序、多个模块及多个线程。

14.如权利要求1所述的方法，其特征在于：所述新的堆栈跟踪显示一像恶意的行为，其中所述像恶意的行为与多个堆栈跟踪有相似之处，其中所述多个堆栈跟踪与一恶意代码相关。

15.如权利要求1所述的方法，其特征在于：所述多个堆栈跟踪模板是基于在一被预定的时段内在所述多个用户上相似的被允许的代码经授权的安装。

16.如权利要求1所述的方法，其特征在于：所述被预定的要求被选择以防止或减少由所述被允许的代码而来的多个被允许的网络连线的一假阳性连线阻挡。

17.如权利要求1所述的方法，其特征在于：所述被预定的要求代表用于多个被允许的网络连线的一假阳性连线阻挡的一容差水平。

18.一种用于认证由一被允许的代码建立一网络连线的一企图的系统，其特征在于：所述系统包含：

具有多个之前被观测的多个堆栈跟踪模板的一数据集，其中所述多个堆栈跟踪模板的每一个代表在多个堆栈跟踪中普遍存在的一堆栈跟踪模式，其中所述多个堆栈跟踪是通过监控多个用户的多个堆栈而记录，其中所述多个用户是在一连线建立过程中执行一被允许的代码，其中所述连线建立过程是用于建立与所述被允许的代码相关的多个网络连线；及

至少一事件管理服务器，包括由所述至少一事件管理服务器的一处理器可实现的一代码，以用于：

接收在多个用户中的一某个新的用户处被记录的一新的堆栈跟踪，其中所述新的堆栈跟踪是由所述某个新的用户在用于一新的网络连线的一新的连线建立过程中纪录；

测量所述新的堆栈跟踪与所述多个堆栈跟踪模板之间的一相似度，以识别一被匹配到的堆栈跟踪模板；

评估所述被匹配到的堆栈跟踪模板，以用于一被预定的规则要求，其中评估所述被匹配到的堆栈跟踪模板的步骤包含：

递增一计数器的一值，其中所述计数器指示从多个不同的用户而来的多个之前堆栈跟踪模板匹配；及

评估所述值是否违反多个匹配的所述被预定的规则要求；及

以所述被匹配到的堆栈跟踪模板来更新一规则集数据库，以认证与多个堆栈模板相关

联的多个新的网络连线建立，其中所述多个堆栈模板与所述被匹配到的堆栈跟踪模板相匹配。

19.如权利要求18所述的系统，其特征在于：所述系统还包含：

至少一闸道服务器，与所述事件管理服务器及与所述多个用户端中的至少一个进行通信，其中所述至少一闸道服务器包括由所述至少一闸道服务器的一处理器可实现的一代码，以用于：

分析所述新的堆栈跟踪以指定所述新的网络连线为怀疑与一恶意代码相关；及

传输所述新的堆栈跟踪至所述事件管理服务器，以用于分析；

接收所述被以所述被匹配到的堆栈跟踪模板更新的规则集数据库；及

允许所述新的网络连线的一连线建立。

20.如权利要求18所述的系统，其特征在于：

所述至少一事件管理服务器与多个闸道服务器进行通信，其中每一个别的闸道服务器与所述多个用户中的至少一个用户进行通信，及每一个别的闸道服务器包括由每一个别的闸道服务器的一处理器可实现的一代码，以：

从所述新的用户接收所述新的堆栈跟踪；

分析所述新的堆栈跟踪以决定建立一恶意通信的一可疑尝试存在或不存在，其中所述网络连线被使用于恶意活动；

当所述新的堆栈跟踪与一恶意数据有相关性时，检测建立用于所述恶意通信的所述网络连线的一企图；及

产生一消息，其中所述消息代表使用所述网络连线建立所述恶意通信的所述可疑尝试；及

所述事件管理服务器的所述代码可被实现以从每一个别的闸道服务器接收所述消息，且进行所述测量的步骤、所述评估的步骤及所述更新的步骤以便重指定所述新的网络连线为代表一被允许的网络连线，而防止或减少多个假阳性网络连线的阻挡，其中所述多个假阳性网络连线是由对于所述个别的闸道服务器而言呈恶意的所述被允许的代码而来。

21.如权利要求20所述的系统，其特征在于：所述某个新的用户还包含与所述被允许的代码相关联的一被允许的应用程序，其中所述被允许的代码包括由所述新的用户的一处理器可实现的一代码，而引起怀疑与一恶意代码相关的识别。

22.如权利要求20所述的系统，其特征在于：所述至少一事件管理服务器及所述多个闸道服务器被组合成所述至少一事件管理服务器。

23.如权利要求18所述的系统，其特征在于：所述被允许的代码被安装为在一应用程序内一被插入的代码，其中所述被插入的代码与一堆栈数据相关联，所述堆栈数据相似于与一恶意被插入的代码相关联的一堆栈数据。

24.如权利要求18所述的系统，其特征在于：所述被允许的代码被配置具有建立一网络连线的一高级权限，相似于一恶意代码获得一高级权限的方式。

25.如权利要求18所述的系统，其特征在于：所述系统还包含：

一用户模块，用于安装在每一个别的用户处，其中所述用户模块包括由所述个别的用户的一处理器可实现的一代码，以用于：

识别在所述个别的用户处一新被安装的应用程序；及

分析所述新被安装的应用程序以识别由所述新被安装的应用程序而来的建立用于一恶意通信的一连线的一尝试。

26.如权利要求25所述的系统,其特征在于:所述新被安装的应用程序被一使用者安装为一被允许的应用程序,其中所述使用者违背一安装策略。

用于恶意代码检测的准确保证的系统及方法

[0001] 相关申请案

[0002] 此申请案主张根据第35号美国法典第119(e)条于2014年11月25日提交申请的美国临时专利申请案第62/083,985号以及于2015年04月14日提交申请的美国临时专利申请案第62/147,040号的优先权,其内容通过引用的方式并入本文整体中。

背景技术

[0003] 本发明,于其一些实施例中,是有关于用于恶意连线检测的多个系统及多个方法,特别是,但非专门是,有关于用于恶意通信检测的准确保证的多个系统及多个方法。

[0004] 某些种类的恶意代码攻击多个计算机且使用所述主计算机以通过一网络连线与多个其它服务器连接。于一示例中,所述网络连线是由所述恶意代码本身所引发,例如,以传送一被窃取的数据至一远程服务器。于另一示例中,所述恶意软件将一代码插入至一正当的应用程序,接着,所述被插入的代码引发至一远程服务器的一连线,以传送一被窃取的数据。

[0005] 一种恶意攻击的一示例为一先进的有针对性的攻击(ATA),所述先进的有针对性的攻击为一复杂的攻击,于所述复杂的攻击中,未经授权的一方获得存取一网络的权限,且保持长时间不被检测到。大多数的先进的有针对性的攻击的意图为窃取数据,而非为对所述网络造成损害。多个先进的有针对性的攻击是针对具有高价值信息的多个行业中的多个组织,所述多个行业例如为多个信用卡服务商、多个政府机关,及金融服务业。

[0006] 多个反先进的有针对性的攻击的解决方案的多个示例是基于所述攻击的检测或所述渗透的恶意代码的检测。于另一示例中,多个其它的工具被设计以检测在行动中的一不正常或恶意活动。

发明内容

[0007] 依据本发明的一些实施例的一方面,一种用于认证由一被允许的代码建立一网络连线的一企图的方法被提供,所述方法包含步骤:提供具有多个之前被观测的多个堆栈跟踪模板的一数据集,其中所述多个堆栈跟踪模板的每一个代表在多个堆栈跟踪中普遍存在的一堆栈跟踪模式,其中所述多个堆栈跟踪是通过监控多个用户的多个堆栈而记录,其中所述多个用户是在一连线建立过程中执行一被允许的代码,其中所述连线建立过程是用于建立与所述被允许的代码相关的多个网络连线;接收一新的堆栈跟踪,其中所述新的堆栈跟踪是在用于一新的网络连线的一新的连线建立过程中被一新的用户记录;测量所述新的堆栈跟踪与所述多个堆栈跟踪模板之间的一相似度,以识别与一堆栈跟踪模板的一匹配;评估所述被匹配到的堆栈跟踪模板,以用于一被预定的规则要求;及以所述被匹配到的堆栈跟踪模板来更新一规则集数据库,以认证与多个堆栈模板相关联的多个新的网络连线建立,其中所述多个堆栈模板与所述被匹配到的堆栈跟踪模板相匹配。

[0008] 可选地,所述多个堆栈跟踪模板被指定为代表所述被允许的代码的一可疑恶意行为。

[0009] 可选地，所述多个堆栈跟踪模板及所述新的堆栈跟踪包括被以与所述被允许的代码的所述堆栈跟踪相关联的方式收集的一上下文数据，及所述相似度是依据所述上下文数据而被测量。可选地，所述上下文数据包括一事件识别码及/或一主机名称。可替换地或额外地，所述上下文数据包括选自由下述组成的群组中的至少一成员：在所述个别的用户处运行的一相似操作系统、一相似被允许的应用程序、多个不同被允许的应用程序的一相似堆栈跟踪数据，及建立所述网络连线的多个相似协议。

[0010] 可选地，所述方法还包含：基于所述匹配的不存在，将所述新的堆栈跟踪加入所述数据集成为一新的堆栈跟踪模板。

[0011] 可选地，评估所述被匹配到的堆栈跟踪模板的步骤包含：递增一计数器的一值，其中所述计数器指示从多个不同的用户而来的多个之前堆栈跟踪模板匹配；及评估所述值是否违反多个匹配的所述被预定的规则要求。可选地，所述多个不同的用户为一相同被指定的群组的一部分。

[0012] 可选地，当所述被匹配到的堆栈跟踪模板及所述新的堆栈跟踪与多个不同的用户相关联时，评估所述被匹配到的堆栈跟踪模板的步骤即被进行，以用于所述被预定的规则要求。

[0013] 可选地，所述方法还包含：分析所述新的堆栈跟踪以指定所述网络连线为怀疑与一恶意代码相关；及所述方法还包含：重指定与所述恶意代码相关的所述怀疑为与所述被允许的代码相关。可选地，与所述恶意代码相关的所述怀疑是由一新的被允许的代码所引起，其中所述新的被允许的代码被安装于显示一像恶意的行为的所述新的用户上。可替换地或额外地，所述被允许的代码代表由不正确地引起怀疑与所述恶意代码相关的所述识别而来的一假阳性识别。可替换地或额外地，所述堆栈跟踪被与至少一堆栈跟踪模板匹配，其中所述堆栈跟踪与所述被认证通过的新的网络连线相关联，及所述至少一堆栈跟踪模板与建立用于一恶意通信的所述网络连线的一企图相关联。

[0014] 可选地，所述新的堆栈跟踪及所述多个堆栈跟踪模板还包含一流动数据，包括选自由下述组成的群组中的至少一成员：多个程序、多个模块及多个线程。

[0015] 可选地，所述新的堆栈跟踪显示一像恶意的行为，其中所述像恶意的行为与多个堆栈跟踪有相似之处，其中所述多个堆栈跟踪与一恶意代码相关。

[0016] 可选地，所述多个堆栈跟踪模板是基于在一被预定的时段内在所述多个用户上相似的被允许的代码经授权的安装。

[0017] 可选地，所述被预定的要求被选择以防止或减少由所述被允许的代码而来的多个被允许的网络连线的一假阳性连线阻挡。

[0018] 可选地，所述被预定的要求代表用于多个被允许的网络连线的一假阳性连线阻挡的一容差水平。

[0019] 依据本发明的一些实施例的一方面，一种用于认证由一被允许的代码建立一网络连线的一企图的系统被提供，所述系统包含：具有多个之前被观测的多个堆栈跟踪模板的一数据集，其中所述多个堆栈跟踪模板的每一个代表在多个堆栈跟踪中普遍存在的一堆栈跟踪模式，其中所述多个堆栈跟踪是通过监控多个用户的多个堆栈而记录，其中所述多个用户是在一连线建立过程中执行一被允许的代码，其中所述连线建立过程是用于建立与所述被允许的代码相关的多个网络连线；及至少一事件管理服务器，包括由所述至少一事件

管理服务器的一处理器可实现的一代码，以用于：接收在多个用户中的一某个新的用户处被记录的一新的堆栈跟踪，其中所述新的堆栈跟踪是由所述某个新的用户在用于一新的网络连线的一新的连线建立过程中纪录；测量所述新的堆栈跟踪与所述多个堆栈跟踪模板之间的一相似度，以识别与一堆栈跟踪模板的一匹配；评估所述被匹配到的堆栈跟踪模板，以用于一被预定的规则要求；及以所述被匹配到的堆栈跟踪模板来更新一规则集数据库，以认证与多个堆栈模板相关联的多个新的网络连线建立，其中所述多个堆栈模板与所述被匹配到的堆栈跟踪模板相匹配。

[0020] 可选地，所述系统还包含：至少一闸道服务器，与所述事件管理服务器及与所述多个用户端中的至少一个进行通信，其中所述至少一闸道服务器包括由所述至少一闸道服务器的一处理器可实现的一代码，以用于：分析所述新的堆栈跟踪以指定所述新的网络连线为怀疑与一恶意代码相关；及传输所述新的堆栈跟踪至所述事件管理服务器，以用于分析；接收所述经更新的规则集数据库；及允许所述新的网络连线的一连线建立。

[0021] 可选地，所述至少一事件管理服务器与多个闸道服务器进行通信，其中每一个别的闸道服务器与所述多个用户中的至少一个用户进行通信，及每一个别的闸道服务器包括由每一个别的闸道服务器的一处理器可实现的一代码，以：从所述新的用户接收所述新的堆栈跟踪；分析所述新的堆栈跟踪以决定建立一恶意通信的一可疑尝试存在或不存在，其中所述网络连线被使用于恶意活动；当所述新的堆栈跟踪与一恶意数据有相关性，检测建立用于所述恶意通信的所述网络连线的一企图；及产生一消息，其中所述消息代表使用所述网络连线建立所述恶意通信的所述可疑尝试；及所述事件管理服务器的所述代码可被实现以从每一个别的闸道服务器接收所述消息，且进行所述测量的步骤、所述评估的步骤及所述更新的步骤以便重指定所述新的网络连线为代表一被允许的网络连线，而防止或减少多个假阳性网络连线的阻挡，其中所述多个假阳性网络连线是由对于所述个别的闸道服务器而言呈恶意的所述被允许的代码而来。可选地，所述某个新的用户还包含与所述被允许的代码相关联的一被允许的应用程序，其中所述被允许的代码包括由所述新的用户的一处理器可实现的一代码，而引起怀疑与一恶意代码相关的识别。可替换地或额外地，所述至少一事件管理服务器及所述多个闸道服务器被组合成所述至少一事件管理服务器。

[0022] 可选地，所述被允许的代码被安装为在一应用程序内一被插入的代码，其中所述被插入的代码与一堆栈数据相关联，所述堆栈数据相似于与一恶意被插入的代码相关联的一堆栈数据。

[0023] 可选地，所述被允许的代码被配置具有建立一网络连线的一高级权限，相似于一恶意代码获得一高级权限的方式。

[0024] 可选地，所述系统还包含：一用户模块，用于安装在每一个别的用户处，其中所述用户模块包括由所述个别的用户的一处理器可实现的一代码，以用于：识别在所述个别的用户处一新被安装的应用程序；及分析所述新被安装的应用程序以识别由所述新被安装的应用程序而来的建立用于一恶意通信的一连线的一尝试。可选地，所述新被安装的应用程序被一使用者安装为一被允许的应用程序，其中所述使用者违背一安装策略。

[0025] 依据本发明的一些实施例的一方面，一种用于认证由一被允许的代码建立一网络连线的一企图的计算机程序产品被提供，所述计算机程序产品包含：多个程序指令，用于提供具有多个之前被观测的多个堆栈跟踪模板的一数据集，其中所述多个堆栈跟踪模板的每

一个代表在多个堆栈跟踪中普遍存在的一堆栈跟踪模式，其中所述多个堆栈跟踪是通过监控多个用户的多个堆栈而记录，其中所述多个用户是在一连线建立过程中执行一被允许的代码，其中所述连线建立过程是用于建立与所述被允许的代码相关的多个网络连线；多个程序指令，用于接收一新的堆栈跟踪，其中所述新的堆栈跟踪是在用于一新的网络连线的一新的连线建立过程中被一新的用户记录；多个程序指令，用于测量所述新的堆栈跟踪与所述多个堆栈跟踪模板之间的一相似度，以识别与一堆栈跟踪模板的一匹配；多个程序指令，用于评估所述被匹配到的堆栈跟踪模板，以用于一被预定的规则要求；及多个程序指令，用于以所述被匹配到的堆栈跟踪模板来更新一规则集数据库，以认证与多个堆栈模板相关联的多个新的网络连线建立，其中所述多个堆栈模板与所述被匹配到的堆栈跟踪模板相匹配。

[0026] 除非另有被定义，本文中所使用的所有的多个技术及/或科学术语有与本发明所属领域的技术人员所公知者相同的意义。虽然与本文中所描述者相似或等同的多个方法与多个题材可被使用以实施或测试本发明的多个实施例，多个示例性的方法及/或多个示例性的题材将于下被描述。在冲突的情况下，包含多个定义的专利说明书将为优先。此外，所述多个题材、所述多个方法及所述多个示例仅为说明性，而非意图为必要地限制性。

附图说明

[0027] 本发明的一些实施例于本文中被以仅为示例的方式参照附图描述。因现将特别详细参照附图，须强调所显示之细节为以示例的方式，且为用于本发明的多个实施例的说明性讨论的多个目的。在这方面，配合附图的说明使得本发明的多个实施例如何可被实施对于本领域的技术人员而言为明白易懂的。

[0028] 于附图中：

[0029] 图1A是依据本发明的一些实施例的一方法的一流程图，所述方法是用于评估一新的网络连线的数据。

[0030] 图1B是依据本发明的一些实施例的一方法的一流程图，所述方法是用于一网络连线的检测的品质保证，所述网络连线是用于恶意通信。

[0031] 图2是依据本发明的一些实施例的一系统的多个元件的一框图，所述系统是用于评估一网络连线的数据，所述评估的步骤是可选地基于用于恶意通信的一网络连线的检测的品质保证。

[0032] 图3A至3B是依据本发明的一些实施例的多个系统体系架构的多个框图，所述多个系统体系架构是基于图2的所述系统。

[0033] 图4A至4B是依据本发明的一些实施例的多个调用堆栈的多个示例。

具体实施方式

[0034] 本发明，于其一些实施例中，是有关于用于恶意连线检测的多个系统及多个方法，特别是，但非专门是，有关于用于恶意通信检测的准确保证的多个系统及多个方法。

[0035] 本发明的一些实施例一方面是有关于一事件管理服务器，所述事件管理服务器基于一被预定的要求，评估一新的网络连线为与一被允许的代码相关，所述被预定的要求定义一匹配的一被测量的相似度，所述匹配是介于与所述新的网络连线相关联的流动数据及

一之前被观测的流动数据(或堆栈跟踪)模板之间,所述之前被观测的流动数据(或堆栈跟踪)模板代表与多个其它网络连线的多个匹配。可选地,所述被预定的要求代表由多个其它用户而来的多个新的网络连线的流动数据之间的多个相似的匹配之前已被与所述相同的模板匹配。当有足够数量的显示相同流动数据的用户已被与所述模板匹配时,所述被匹配到的模板被所述事件管理服务器认证通过,以允许多个新的网络连线的建立。所述多个用户可属于一相同的预被指定的群组,例如,一组织、一公司、一部门,及一团队。所述流动数据可发生于相同或相似的上下文数据内。基于所述被预定的要求的所述认证的步骤可例如于所有所述相同的群组中的多个用户均安装相同的被允许的代码时发生。

[0036] 可选地,所述事件管理服务器认证由被允许的代码产生的流动数据,由所述被允许的代码产生的所述流动数据被怀疑有用于恶意活动的多个网络连线的建立。当所述相同(或相似的)看似恶意的流动数据被在多个不同的用户处观测到时,所述可疑流动数据被重指定为被认证通过的流动数据,所述被重指定的步骤例如是通过更新定义被允许的流动数据的一规则集数据库来进行。

[0037] 所述事件管理服务器可选地与一或多个闸道器进行通信,每一闸道器与一或多个用户端进行通信。多个堆栈跟踪的多笔记录及/或与新的未知的代码相关联的流动数据被在一新的用户处分析,所述新的未知的代码与一新的网络建立过程相关,所述被分析的步骤是通过测量与一之前被观测的流动数据模板的一相似度相关性以决定所述新的堆栈跟踪是与被允许的代码相关联为何时发生来进行。所述流动数据模板代表从多个其它不同的用户而来的一或多个之前被观测的相似的流动数据。之前的匹配的数量可被存储于一计数器内。当匹配的数量超过所述被预定的要求时,所述被匹配到的流动数据模板被认证通过。与所述被认证通过的模板匹配的新的流动数据(其与多个新的网络连线建立企图相关)被允许继续进行所述连线建立。

[0038] 于一些实施例中,与所述被允许的代码相关联的所述多个新的连线建立过程的相关联的步骤是以两阶段进行。一第一阶段(其可被与所述多个用户进行通信的所述闸道服务器进行)识别在用户处由所述未知的代码建立用于一恶意通信的一网络连线的一可疑企图。一第二阶段(其可被与所述多个闸道服务器连接的所述事件管理服务器进行)使用之前匹配所引起的事件及其多个个别的流动数据模板进行保证品质的步骤,以决定是否所述可疑企图实际上与被允许的代码相关,而因此为安全的。当一事件及其个别的流动数据模板被认证通过时,一新的规定被加入所述多个闸道器的所述数据库,以允许被所述流动数据模板识别出的且与所述事件相关的多个未来的连线建立。

[0039] 可选地,在所述可疑连线企图先被识别出后,所述认证所述可疑连线流动数据的步骤被以额外处理的方式进行。被识别出为可疑的所述连线建立的子集可为保证品质进一步被处理,以确保所述连线建立实际上与恶意代码相关而非与被允许的代码(例如,应用程序及/或模块)相关。如此,所述保证品质的处理对于所述可疑企图的子集而言是被中央进行,而多个正常的连线建立模式的多个指定(例如,在一本地闸道服务器处被进行)可被本地进行。

[0040] 在所述第一状态中,起源于多个个别的用户端处的多个连线建立被在一或多个闸道服务器处监控,所述被监控的步骤是基于多个被连接的用户中的每一个传输数据至所述闸道服务器以用于分析的步骤来进行,所述数据代表与所述连线建立过程相关的流动数

据。在所述第二阶段中，当所述闸道服务器决定所述连线建立因与恶意活动相关联而为可疑时，与所述一或多个闸道服务器进行通信的一事件管理服务器分析与所述被识别出的可疑企图相关联的所述数据，所述事件管理服务器的所述分析的步骤是通过鉴于所述被预定的要求而与之前被引起的匹配规则及其个别的流动数据模板进行匹配，以决定所述企图实际上为被允许的行为(例如，一假阳性识别)为何时发生来进行。可选地，恶意活动的多个不正确的识别被更正以代表正常行为。

[0041] 所述可疑企图是基于起初与恶意代码感染有相关性的数据分析而被识别出。与引发所述可疑网络连线的所述代码相关的流动数据被分析以决定所述可疑企图是由被允许的正常代码所产生为何时发生，所述被允许的正常代码产生呈现由恶意代码所产生的数据，而不是产生呈现正常的数据或数据流。所述可疑企图可接着被所述事件管理服务器核实，所述事件管理服务器可更正所述企图的不正确的分类，而为实际上与被允许的代码相关(及非与原本所指定的恶意代码相关)。所述网络连线可基于所述事件管理服务器的所述多个结果而被激活，所述网络连线起初可被所述第一闸道器分析不正确地阻挡。所述网络连线可在多个后续相似的事件被识别出及被匹配到时被激活，如本文所述。应注意的是，可有两个操作模式。一第一操作模式，如上所述，在所述第一事件被观测到(而认为所述事件与恶意活动相关)时，阻挡所述网络，及在多个额外的相似的事件被观测到时，激活所述网络。一第二操作模式可一开始以一模拟模式操作，以训练所述系统仅通过观测而认出多个事件而不干涉网络激活及/或阻挡。

[0042] 如此，假阳性连线阻挡被防止或被减少，以允许由所述被允许的代码建立多个连线。通过检测所述可疑尝试实际上不与恶意代码相关但与被允许的及/或正常代码(其显示像恶意的行为)相关的发生，与恶意通信相关的多个可疑连线建立尝试的识别中的多个错误被防止或被减少。

[0043] 在详细解释本发明的至少一实施例前，应理解本发明非必要地将其应用限制在以下之说明中所陈述及/或在附图及/或示例中所显示的所述多个元件及/或多个方法的所述多个构造的细节及所述安排。本发明能够有多个其它的实施例或能够被以各种方式实施或实行。

[0044] 本发明可为一系统、一方法及/或一计算机程序产品。所述计算机程序产品可包括一计算机可读存储介质(或多个计算机可读存储介质)，所述计算机可读存储介质有多个计算机可读程序指令于其上，以用于使一处理器实行本发明的多个方面。

[0045] 所述计算机可读存储介质能够为一有形设备，所述有形设备能够保持及存储多个指令，以供一指令执行设备使用。所述计算机可读存储介质可为，例如，但不限于为，一电子存储设备、一磁存储设备、一光学存储设备、一电磁存储设备、一半导体存储设备，或前述的任何适当的组合。所述计算机可读存储介质的多个较具体的示例的一非穷尽的清单包括以下：一便携式计算机软盘、一硬盘、一随机存取存储器(RAM)、一只读存储器(ROM)、一可擦除可编程只读存储器(EPROM或闪存)、一静态随机存取存储器(SRAM)、一便携式光盘只读存储器(CD-ROM)、一数字多用盘(DVD)、一闪盘、一软盘，或前述的任何适当的组合。一计算机可读存储介质，如本文中所使用，不是被解释为多个瞬时性的信号本身，例如多个无线电波或多个其它自由传播的电磁波、传播通过一波导管或多个其它传输介质的多个电磁波(例如，穿越通过一光纤电缆的多个光脉冲)，或被传输通过一电线的多个电信号。

[0046] 本文中所述的多个计算机可读程序指令能够从一计算机可读存储介质被下载至多个分别的计算/处理设备，或经由一网络下载至一外部计算机或外部存储设备，所述网络例如为一互联网、一局域网络、一广域网络及/或一无线网络。所述网络可包含多条传输用铜电缆、多条传输用光纤、无线传输、多个路由器、多个防火墙、多个交换器、多个闸道计算机及/或多个边缘服务器。在每一计算/处理设备中，一网络适配卡或网络接口从所述网络接收多个计算机可读程序指令，并前送所述多个计算机可读程序指令，以用于存储在所述分别的计算/处理设备内的一计算机可读存储介质中。

[0047] 用于实行本发明的多个操作的多个计算机可读程序指令可为多个汇编指令、多个指令集架构(ISA)指令、多个机器指令、多个机器相关指令、微代码、多个固件指令、一状态设置数据，或以一种或多种编程语言的任何组合编写的源代码或目标代码，所述编程语言包括一面向对象的编程语言，例如Smalltalk、C++等，及多种常规的过程式编程语言，例如"C"语言，或多种类似的编程语言。所述多个计算机可读程序指令可完全地在所述使用者计算机上执行、部分地在所述使用者计算机上执行、作为一个独立的软件包执行、部分在所述使用者计算机上及部分在一远程计算机上执行，或完全在所述远程计算机或服务器上执行。在涉及所述远程计算机的情形中，所述远程计算机可通过任何种类的网络，连接到所述使用者计算机，所述任何种类的网络包括一局域网络(LAN)或一广域网络(WAN)，或者，可连接到一外部计算机(例如使用一互联网服务提供商来通过一互联网连接)。在一些实施例中，通过利用所述多个计算机可读程序指令的状态信息而个性化所述电子电路，所述电子电路例如为可编程逻辑电路、现场可编程口阵列(FPGA)或可编程逻辑阵列(PLA)，所述电子电路可执行所述多个计算机可读程序指令，从而进行本发明的多个方面。

[0048] 本文参照依据本发明的多个实施例的多个方法、多个装置(系统)和多个计算机程序产品的多个流程图例证及/或多个框图描述了本发明的多个方面。应当理解，所述多个流程图例证及/或所述多个框图的每一方框及所述多个流程图例证及/或所述多个框图中多个方框的多个组合，都能够由多个计算机可读程序指令执行。

[0049] 运些多个计算机可读程序指令可被提供给一通用计算机、一专用计算机或一其它可编程数据处理装置的一处理器，以产生一种机器，以致于所述多个指令在经由所述计算机或所述其它可编程数据处理装置的所述处理器执行时，创建了实现所述流程图及/或所述框图中的一个或多个方框中规定的所述多个功能/所述多个动作的装置。运些计算机可读程序指令也可被存储在一计算机可读存储介质中，运些计算机可读程序指令能够使得一计算机、一可编程数据处理装置及/或多个其它设备以一特定方式工作，以致于有指令被存储于其中的所述计算机可读存储介质包括一个制造品，所述制造品包括实现所述流程图及/或所述框图中的一个或多个方框中规定的所述多个功能/所述多个动作的多方面的多个指令。

[0050] 所述多个计算机可读程序指令也可被加载到一计算机、一其它可编程数据处理设备、或一其它设备上，以使在所述计算机、所述其它可编程设备或所述其它设备上进行一系列操作步骤，以产生一计算机实现的过程，以致于在所述计算机、所述其它可编程设备或所述其它设备上执行的所述多个指令实现所述流程图及/或所述框图中的一个或多个方框中规定的所述多个功能/所述多个动作。

[0051] 附图中的所述流程图和所述多个框图显示了依据本发明的不同实施例的多个系

统、多个方法和多个计算机程序产品的可能实现的体系架构、功能和操作。在这方面，所述流程图或所述多个框图中的每个方框可代表一模块、一程序段或多个指令的一部分，所述模块、所述程序段或所述多个指令的所述部分包含用于实现规定的逻辑功能的一或多个可执行指令。在一些替换的实现中，在所述方框中被标注的多个功能可不同于在附图中被标注的顺序发生。例如，两个被连续显示的方框实际上可实质并行地被执行，或所述两个方框有时也可按相反的顺序被执行，依照被涉及的所述功能而定。也要注意的是，所述框图及/或所述流程图例证中的每个方框、及在所述框图及/或所述流程图例证中的多个方框的多个组合，能够由多个专用的基于硬件的系统来实现，所述多个专用的基于硬件的系统进行所述多个被规定的功能或动作，或实现多个专用硬件与计算机指令的多个组合。

[0052] 如本文中所述，术语「流动数据」是指在所述用户端处被收集的数据，所述数据包括所述调用堆栈数据及可选地一或多个调用堆栈相关数据项目，如程序数据、模块分析数据及线程数据。术语「流动数据」及「调用堆栈数据」有时为可互换的。

[0053] 如本文所定义，术语「连线建立」是指在所述被允许的代码能通过一网络连线传输及/或接收数据前发生的所述多个被计算机化的过程。所述连线建立过程可被从所述正常代码接收多个引发命令的一应用编程接口管理及/或执行，以建立所述连线、从所述正常代码接收数据而通过所述已建立的连线传输，及/或通过所述已建立的连线传输所接收的数据至所述正常代码。

[0054] 现参照图1A，其是依据本发明的一些实施例的一方法的一流程图，所述方法是用于可选地鉴于上下文数据而评估一网络连线的流动数据。亦参照图2，其是依据本发明的一些实施例的一系统，所述系统是用于认证一新的网络建立过程。参照图2所描述的所述系统可执行参照图1B所描述的所述方法。

[0055] 所述多个系统及/或方法收集看似恶意的行为，当所述看似恶意的行为被在多个用户处观测到时，所述看似恶意的行为暗示恶意活动的不正确的检测。所述恶意行为被重指定为被允许的行为。所述多个系统及/或方法是基于一流动数据模板而将新的未知的代码识别为被允许的，所述流动数据模板是基于见于多个其它用户的多个共同的模式而被创建。所述多个共同的模式被假定是由所述相同(或相似的)被允许的代码所产生。当所述新的数据被与流动数据模板比对及匹配时，与所述新的数据相关的所述未知的代码被指定为一被允许的代码，所述被允许的代码即为被使用来训练所述模板的相同或相似的被允许的代码。

[0056] 每一被安装的代码的多个外部指定(例如，为被允许的及/或恶意的)非为被要求的。所述多个系统及/或方法在见到多个共同的模式时，自动指定代码为被允许的，及在一新的数据与所述已学习的流动数据模板有相关性时，自动指定一新的未知的代码为被允许的。所述被安装的代码自动通过本文所述的所述多个系统及/或方法被指定为被允许的，而非必要地要求每一代码被一外部实体预指定。例如，一系统管理员不需要验证所述代码。可替换地，手动干预可被允许，例如，以手动更正识别及/或匹配多个事件中的多个错误，及/或指定一代码为被允许，及/或指定一代码为恶意中的多个错误，或多个其它更正。所述手动干预被授予，例如，所述系统、所述方法、及/或一计算机程序产品的管理员。

[0057] 用于被允许的代码的指定及/或用于检测用于所述恶意通信的一网络连线的品质保证的所述系统可被安装于一系统200内。

[0058] 所述系统200包括至少一用户202，所述用户202例如为一笔记本计算机、一台式计算机、一移动设备(例如，一智能手机、一平板计算机)及/或一服务器。所述用户202为一终点用户，所述终点用户能够引发一新的网络连线，所述新的网络连线是用于来自所述用户202及/或至所述用户202的一数据传输。所述终点用户202可为一服务器。

[0059] 所述用户202包括多个网络连线能力，所述多个网络连线能力例如为一网络接口、一发送器，及/或一接收器。所述用户202可通过一或多个网络206与一正当远程服务器204通信，所述一或多个网络206例如为一无线网络、一有线网络、一蜂窝网络、一互联网、一私有网络，及其多个网络的多个组合。

[0060] 可选地，一终点模块208A被安装在所述一或多个用户202的一存储器上或与所述一或多个用户202通信，(例如，被预先安装、被与在所述用户上运行的一操作系统整合，及/或从一远程服务器或一本地存储器下载且被本地安装)。可选地，所述终点模块208A包含一代码，所述代码包括多个程序指令，所述多个程序指令是用于被所述用户202的一处理器实现，及用于监控在所述用户202上的一连线建立相关活动，如本文所述。可替换地或额外地，所述模块208A进行由一闸道器210及/或事件管理服务器216下指示的多个功能，例如，以阻挡所述被企图的网络建立连线、以停止所述连线建立过程、及/或以激活所述连线。

[0061] 事件管理服务器216在连线建立过程中从多个用户202接收与多个应用程序相关的数据(例如，被封装于多个封包及/或多个帧中的多个网络消息)；分析所述数据以用于多个之前被观测的被聚合的共同的模式；评估所述多个被聚合的观测以用于一被预定的要求；及基于所述流动数据模板而产生一套规则，所述流动数据模板定义与多个被允许的应用程序相关的数据。事件管理服务器216可选地使用一聚合模块218。当一连线建立过程是与未知的代码相关时，一闸道器210应用所述一套规则224，所述一套规则224包括所述多个新的规则，以指定所述未知的代码为所述被允许的代码，及允许所述新的网络连线的建立。

[0062] 应注意的是，图1A的一方法描述集中在所述事件管理服务器216内的多个过程的一方法，而图1B描述跨所述多个系统的所述多个元件的一总体的方法。

[0063] 在102中，一数据被在事件管理服务器处接收，所述数据是与在用于建立一网络连线的一连线建立过程中的一代码的一流动数据(例如，在一或多个堆栈跟踪中的多笔记录)相关。数据可被通过一网络连线以多个网络消息的形式传输，所述多个网络消息例如是被封装于多个封包及/或多个帧中。可选地，所述数据是可选地由在每一个别的用户202处的终点模块208A本地收集，在每一个别的用户202处的终点模块208A包括由所述用户的所述处理器可实现的一代码。可选地，所述数据被从每一用户经由多个个别的闸道器传输至所述管理服务器(每一闸道器与一组用户进行通信，及与所述管理服务器进行通信，如本文所述)。

[0064] 可选地，与所述网络连线建立企图相关的事件识别码(ID)及/或主机数据被终点模块208A本地收集。主机数据的多个示例包括下述的一或多个：使用者名称、公司名称、公司部门、公司团队、其它组织的内部群组名称、虚拟机器名称，及与所述多个网络连线建立企图相关的多个网络地址，所述多个网络地址例如为所述用户机器的地址及所述被允许的代码的地址。事件ID的多个示例可包括：被引起的恶意规则识别、在所述个别的用户设备处所运行的所述操作系统、所述被允许的应用程序、所述被安装的被允许的模块，及在建立所述网络连线的所述企图中所使用的所述通信协议(例如，传输控制协议(TCP))。

[0065] 可选地，所述被收集的数据被传输至事件管理服务器216。可替换地或额外地，所述被收集的数据先被传输至闸道器210，如参照图1B所述。

[0066] 每一用户202已于其上安装被允许的代码208C，所述被允许的代码208C与所述连线建立过程相关联。

[0067] 被允许的代码208C，例如一被允许的应用程序及/或一被允许的模块，被安装于用户202内，所述安装的步骤是，例如由一网络管理员手动及/或基于多个权限而自动进行。被允许的代码208C引发多个连线建立尝试以建立及激活一网络连线。

[0068] 被允许的代码208C可被编程而具有不好的做法的连线建立数据，所述不好的做法连线建立数据与多个被恶意代码感染的应用程序的连线建立数据相似。

[0069] 被允许的代码208C可为一独立的应用程序，例如一被定制的及/或公司内部的应用程序。多个定做的及/或公司内部的应用程序可被设计以满足多个组织的特别的要求及/或解决软件部署中的差距。在一企业部门单元中，多个公司内部的应用程序可被创建及/或定制以满足在一特定业务上一关键的业务功能。被设计以用于多个特别的内部要求的软件可使用多个非标准的方法，例如代码插入，来以与恶意代码所使用的多个方法相似的方式干预连线建立。于另一示例中，代码208C可为一被允许的定制保安审计及/或强制应用程序，所述被允许的定制保安审计及/或强制应用程序跨多个公司用户(例如，多台台式计算机、多台笔记本计算机及多台服务器)强制多个公司策略的遵守。所述保安应用程序可经授权而为侵入性的，经授权而涉及连线劫持，及/或经授权以进行多个其它强制方法，所述多个其它强制方法与恶意代码所进行的多个方法相似。

[0070] 代码208C可为一模块，所述模块被以与在用户202上一现有的应用程序相关联的方式安装，例如被安装为一插件、一修补程序及代码插入。例如，模块208C可为一保安工具，所述保安工具被设计以用于受信任的浏览。模块208C可通过插入代码至一现有的网页浏览器以操纵多个网络连线通信而被安装于所述网页浏览器内。所述代码插入是以相似于基于代码插入的恶意代码运作的方式而被进行。所述被插入的代码产生所述连线建立引发应用程序的流动数据，所述连线建立引发应用程序的所述流动数据与具有被恶意插入的代码的一应用程序的流动数据相似。

[0071] 代码208C可与一应用编程接口相关，所述应用编程接口例如为一套接口，所述套接口依据一互联网协议的一传输控制协议(TCP)管理所述连线建立。

[0072] 可选地，所述流动数据是从一调用堆栈及/或多个其它数据来源获得，所述调用堆栈与企图建立所述网络连线的所述应用程序相关，例如是从在存储器中的多个有关位置复制，所述存储器与执行在所述堆栈中的所述多个指令的所述处理器相关联。所述堆栈跟踪包括在所述调用堆栈中的多个程序的多个顺序的数据及/或一或多个快照，所述调用堆栈与所述连线建立相关。例如，所述堆栈跟踪包括在所述跟踪被获得时于所述调用堆栈中的所述多个模块。所述多个模块可基于在所述调用堆栈中的多个代表而被导出，所述多个代表例如为在所述调用堆栈中的指向所述多个模块的多个指针。

[0073] 一或多个堆栈跟踪可在所述请求期间、在引发所述连线建立过程期间及/或在所述连线建立过程中的一或多个点位被获得。在所述连线建立过程中的多个点位被采集的所述多个堆栈跟踪是被选择以采集在所述堆栈中的多个改变，所述多个改变发生在所述请求期间及/或所述连线建立过程中。

[0074] 可选地，在104中，从每一用户所接收的所述流动数据被依据上下文分类，可选地，所述分类的步骤是由服务器216的聚合模块218进行，所述服务器216的所述聚合模块218包括由所述服务器216的所述处理器可实现的代码。所述上下文是基于所述事件ID，可选地包括所述主机数据。所述上下文可帮助决定所述流动数据为恶意的为何时发生及所述流动数据为被允许的为何时发生。例如，当一网络浏览器被加载时，所出现的流动数据可为恶意的，而当一被定制的组织专属应用程序被加载时，所出现的相同(或相似的)流动数据可为安全的。于另一示例中，在相同的主机处被观测到的重复的流动数据可为恶意的，而在多个不同的主机处被观测到的相同(或相似的)流动数据可为安全的。

[0075] 可选地，所述上下文包括一被预定的时段，例如，一天的一个钟头、一个礼拜的一天，或某个日期。可选地，当所述流动数据在所述相同的被预定的时段内被接收时，分类被进行。所述时段可被选择以代表在多个用户上所述代码的推出及安装。应注意的是，与在所述时间上下文外的一时段相关联的流动数据可代表多个感染的模式，而不是被允许的安装。

[0076] 所述上下文数据可帮助将流动数据代表恶意通信的发生与流动数据代表被允许的行为的发生区分。上下文数据可被以与所述被识别出的连线建立流动数据相关联的方式收集。上下文数据的多个示例包括下述的一或多个：在个别的用户处所运行的操作系统；在个别的用户处所运行的多个已知被允许的应用程序；与流动数据有高度相关性(例如，高于一阈值)，所述流动数据与多个不同的被允许的应用程序相关联；及被使用于建立所述网络连线的所述企图中的通信协议。例如，在多个不同的用户上相同(或相似的)操作系统下所执行的多个不同应用程序可产生相似的上下文数据下相似的流动数据。所述流动数据被指定为与被允许的行为相关，所述被允许的行为是由多个被允许的应用程序所允许。

[0077] 在106中，与在某个用户202处的一新的连线建立企图相关联的新的代码的新的流动数据被传输至事件管理服务器216。所述新的流动数据可选地被聚合模块218分析，所述聚合模块218包括由服务器216的所述处理器可实现的代码。所述新的流动数据与多个被存储的之前被观测的流动数据模板之间的一相似度(例如，相关性)被测量，以识别与一流动数据模板的一匹配，所述多个被存储的之前被观测的流动数据模板可被以数据集的形式存储于与服务器216进行通信的一存储器上。例如当相似度的所述相关性为高于一相关性阈值时，所述新的流动数据被匹配到。应注意的是，所述流动数据与模板非必要地需要完全匹配，而仅需足够的相似，如相关性阈值所定义。

[0078] 可选地，所述相似度是依据一恶意规则被测量，所述恶意规则引起所述可能恶意的事件的所述识别，及流动数据的被收集，例如，与所述应用程序相关的一流动数据的数据集已被识别出为可能与恶意活动相关。

[0079] 可替换地或额外地，所述相似度是依据所述上下文数据被测量。所述新的流动数据被与具有相同或相似的上下文数据的一流动数据模板的子集比对，以识别所述子集中的一匹配。如此，可匹配但却为无关的多个其它模板可以先验被排除。发生在多个其它上下文中的多个被匹配到的模板可代表恶意行为，而不能在发生于一不同的上下文中时被排除。

[0080] 可替换地或额外地，所述相似度是依据多个堆栈跟踪专属细节的相似度被测量，所述多个堆栈跟踪专属细节是介于从所述用户所收集的所述堆栈跟踪与所述之前被观测的事件的所述堆栈跟踪之间，所述多个堆栈跟踪专属细节例如为堆栈的种类及所述堆栈中

的多个模块。

[0081] 可选地，匹配是以一阶层的方式逐步被进行，以通过先匹配所述被引起的恶意规则，接着匹配所述上下文，及接着再匹配所述堆栈跟踪数据来增进处理的效能。可替换地，匹配是同时被进行，例如是通过一分类器或一套规则进行，所述分类器或所述一套规则将所述被引起的恶意规则、上下文及堆栈跟踪数据映射至某个事件。

[0082] 可选地，在107中，当没有匹配被找到时，所述新的流动数据是以一新的流动数据模板的形式被由服务器216的所述处理器可实现的代码存储。所述新的流动数据模板接着被与新被接收的流动数据匹配。可替换地或额外地，所述新的流动数据模板是基于多个预设的定义。例如，一管理员可手动定义某个流动数据模板为代表被允许的行为。

[0083] 可替换地，在108中，当一被匹配到的流动数据模板被找到时，所述被匹配到的流动数据模板被评估以用于一被预定的要求，所述评估的步骤可选地是由聚合模块218进行。所述评估的步骤可被设定以满足一或多个规则要求。可选地，每一恶意规则是与其本身的被预定的要求相关联。所述被预定的要求可例如为一阈值、一范围及/或一函数。

[0084] 可选地，所述被预定的要求代表为验证所述相关联的模板要观测到的多个匹配。一计数器可选地可在每有不同的主机数据的匹配时被递增，所述计数器指示之前被观测到的匹配的数量。可替换地，多个其它的计数方法例如基于之前的匹配的数量而可被计算的一函数可被使用。所述计数器的一值被与所述被预定的要求比对，以决定所述值符合或超出所述被预定的要求，例如落入所述范围内、为所述函数所定义、及/或符合或超出所述阈值，为何时发生。

[0085] 可选地，已被匹配的所述新的流动数据可被以与所述被匹配到的模板相关联的方式存储于一数据集中。存储一套的多个流动数据可例如当多个不同的变化被观测到时，让所述模板有多个周期性(或连续性)的更新。可替换地或额外地，所述一套的多个流动数据可被重聚合至所述被更新的模板内。可替换地或额外地，所述一套流动数据的多个成员可代表在所述被匹配到的模板中多个被允许的变化，例如以考虑本地用户的多个配置，所述多个配置例如是所述代码及/或所述操作系统的多个不同的版本。所述计数器值可通过进行所述数据集的所述多个成员的计数而被获得。

[0086] 可选地，所述要求为静态的，例如为一绝对数，所述绝对数例如是在验证所述被匹配到的模板前要被观测到的从相同的群组中多个不同的用户而来的匹配的数量。可替换地或额外地，所述要求为动态的，所述要求可依据多个基本的变数被改变。例如，要被与相同的模板匹配的所述群组中的多个用户的一百分比。所述百分比可保持相同，而匹配的数量则可依所述群组中用户的总数调适，所述群组中用户的总数可因多个新的用户被加入而随时间的推移改变。于另一示例中，所述要求为一或多个保安相关指标的一函数，所述一或多个保安相关指标的所述函数可被计算以用于所述上下文，所述上下文例如是与所述通信协议所提供的保安保护相关、为一部门工作的多个员工的保安级别、及所述连接的应用程序或操作系统的多个已知保安的故障。

[0087] 所述要求可被(例如，一系统管理者)手动预定，被(例如，从一或多个变数计算的一算法)自动定义，及/或从一外部来源获得(例如，从一中央服务器下载)。

[0088] 应注意的是，所述计数器值及/或要求可依据所述上下文被定义。可选地，所述多个不同的用户具有相同的上下文，例如相同的被指定的群组。如此，在相同的群组(例如，相

同的公司、相同的部门、相同的团队)的多个不同的用户中被观测到的相同(或相似的)流动数据代表被允许的行为,例如是由于在相同的群组的多个用户上的一软件安装。在相同的群组的多个用户中所被观测到的相同的流动数据较在多个不同的组织的多个不同的用户中所被观测到的相同的流动数据可能为被允许的行为,所述多个不同的组织的所述多个不同的用户中所被观测到的所述相同的流动数据较不可能是由于被相同的实体安装的共同的软件。

[0089] 可选地,多个不同的要求被选择以用于多个不同的上下文。可选地,当相同的模板被匹配到时,多个不同的要求被选择以用于多个不同的上下文。所述多个不同的要求可代表,例如多个不同的所需保安级别以用于不同的上下文,所述多个不同的所需保安级别例如为用于一公司的一般文书人员的一低保安级别,及用于所述公司的财务人员的一高保安级别。

[0090] 可选地,所述要求可依据一机率值被选择,所述机率值代表所述要求的一置信度,所述要求代表被允许的行为。所述要求可被(手动或自动)选择以防止或减少多个被允许的网络连线的假阳性连线阻挡。一高的要求可在确定性高的多个情况下将多个之前恶意的企图标记为是安全的。例如当恶意活动不能被容忍时,所述高的要求可被选择,即便是以阻挡某些安全的程序(应注意的是,所述多个安全的程序可被手动批准以进行未来的连线建立)为代价,例如在一组织具有敏感的资料的情况下,所述组织例如为一军事设施。一低的要求可在确定性低的多个情况下将多个之前恶意的企图标记为是安全的。在一组织中,所述低的要求可例如在多个被定制的程序为关键且代表所述组织的多个计算机上的重要活动时被选择。

[0091] 可选地,当尚未符合所述要求时,在109中,当所述匹配是对于一新的用户被观测到(即,没有多个之前的匹配)时,所述计数器值被由服务器216的所述处理器可实现的代码递增。与相同的用户相关联的多个重复的匹配不进一步递增所述计数器,例如以避免计数到由所数相同的用户的相同应用程序而来的多个重复的连线建立企图。如此,具有相同(或相似的)流动数据的多个不同的用户的数量被计数。当有足够的具有相同流动数据的多个不同的用户被观测到(如所述要求所定义)时,所述流动数据被认证通过,如在110中。

[0092] 应注意的是,所述计数器是基于从多个用户所接收的流动数据而被递增,其中每一个别的用户执行相似的被安装的代码。从所述多个个别的用户而来的流动数据的相同、相似或有高度相关性(例如,高于一阈值)代表所述被执行的代码被验证通过及/或被允许。所述代码(及/或相关的流动数据)被自动指定为代表被允许的行为,及便是当从每一用户所接收的流动数据会除此以外被指定为代表多个恶意通信的企图时。如此之场景可例如在以一非传统的方式编写的被定制的代码被以一被允许的方式安装在多个公司的计算机时发生,所述非传统的方式例如是没有按照良好的惯例。所述代码呈现恶意,但实际上为被允许的代码。

[0093] 可替换地,当已符合所述要求时,在110中,以所述被匹配到的流动数据模板来更新一规则集数据库,所述更新的步骤是通过由服务器216的所述处理器可实现的代码来进行。与所述被匹配到的流动数据模板相关联的多个新的网络连线企图可被认证通过,且被允许建立多个连线。

[0094] 可选地,由事件管理服务器216所产生的所述多个新的规则可被通过网络连线传

输至用户202，或至多个其它网络设备，例如闸道器210。与每一闸道器210相关联的所述一套规则224可被更新。由未来的流动数据而来的所述连线建立过程被允许被建立，以用于通过网络进行数据传输，所述未来的流动数据是从相同(或相似的)被允许的代码而来。

[0095] 可替换地，当所述未知的代码的所述流动数据没有与任何流动数据模板有相关性时，指示有可疑恶意通信企图的一消息可被产生及被传输。进一步的动作可被进行，例如以阻挡所述连线建立企图，及/或指定所述未知的代码为恶意的。

[0096] 可选地，在112中，所述方法被迭代进行以分析多个新的连线建立企图。

[0097] 现参照图1B，其是依据本发明的一些实施例的一计算机实现的方法的一流程图，所述方法是用于一网络连线的检测的品质保证，所述网络连线是用于恶意通信及/或活动。亦参照图2，其是依据本发明的一些实施例的一系统，所述系统是用于一网络连线的检测的品质保证，所述网络连线是用于恶意通信及/或活动。参照图2所描述的所述系统可执行参照图1B所描述的所述方法。

[0098] 所述多个系统及/或方法为一被识别出的建立所述网络连线的可疑企图提供品质保证，以决定由所述用户上的所述代码所引发的所述连线建立为实际上与恶意活动相关联的发生，或由所述代码所引发的所述连线建立为与被允许的及/或正常的活动相关联的发生，所述用户上的所述代码例如为应用程序、更新模块、插件、及修补程序。所述代码可为正常代码，所述正常代码产生可疑流动数据，所述可疑流动数据与由恶意代码所产生的流动数据相似。如此，基于正常代码而被建立的多个被允许的网络连线被激活，而不是错误地由于所述被识别出的可疑的像恶意的流动数据被阻挡。

[0099] 所述多个系统及/或方法产生多个新的规则，以允许被本地安装的正常代码的流动数据，所述正常代码以与恶意代码相似的方式操作，但实际上却不是恶意代码。例如，基于不好的做法的连线建立而被编程的代码及/或多个应用程序、被编程以满足多个组织的特别的要求的多个被定制的及/或公司内部的模块及/或应用程序、被设计以具有多个管理权限的一高级别的多个软件修补程序及模块。在如此的多个情况中，本文所述的所述多个系统及/或方法进行与恶意代码相关联的流动数据及与被允许的及/或正常代码(其表现得像恶意代码)相关联的流动数据之间除此以外将难以区分的区分。

[0100] 本文所述的所述多个系统及/或方法通过加入一额外的品质保证措施而增进网络效能，所述额外的品质保证措施防止及/或减少不适当的阻挡或关闭多个网络连线。

[0101] 本文所述的所述多个系统及/或方法区分多个实际的恶意连线企图与不正确地被标示的正常的连线建立，而非必要地要求所述特别的恶意代码及/或特别的正常代码的知识。

[0102] 闸道器210从用户202接收连线建立相关数据、分析所述数据，及识别建立用于恶意通信及/或活动的所述网络连线的一可疑企图。可选地，闸道器210为一代理服务器，所述代理服务器作为在用户202上的某个应用程序与一接口之间的一中介设备，用户202的所述某个应用程序引发建立所述网络连线，及所述接口控制建立所述网络连线。闸道器210的额外细节可例如参照美国临时专利申请案号62/083,985被找到。

[0103] 事件管理服务器216与一或多个闸道器210进行通信。服务器216从一或多个闸道器210接收与所述被识别出的可疑企图相关的数据，并决定所述可疑企图为与正常代码相关联何时发生，及可选地所述多个可疑企图为实际上与恶意代码相关联何时发生。事件管

理服务器216产生一信号至所述个别的闸道器210及/或至模块208A，而指出所述可疑企图为假阳性。所述信号可为新的或被更新的一套规则，所述新的或被更新的一套规则将被安装在闸道器210所使用的一套规则224内，以验证及允许多个连线建立。

[0104] 可选地，与事件管理服务器216的一使用者接口222相关联的事件管理服务器216的一管理模块220允许一使用者进行一或多个管理及/或监控功能，所述一或多个管理及/或监控功能例如为多个配置、多个更新、活动、及/或事件的审查。多个使用者可例如借助一网页浏览器通过一网络连线存取使用者接口222。多个用户及/或闸道器及/或事件管理服务器的数据，或每个用户及/或闸道器及/或事件管理服务器的数据可被中央查看及/或分析。

[0105] 现参照图3A至3B，其是依据本发明的一些实施例的多个系统体系架构的多个示例的多个框图，所述多个系统体系架构是基于图2的系统200。

[0106] 图3A绘示一系统300的一体系架构，于所述系统300中，一事件管理服务器320与多个闸道服务器310通信。每一闸道服务器310与多个用户302通信。系统300可被设计，例如以用于一大组织，在所述大组织中，每一闸道器310为被指定的一群组的用户302服务(例如，按部门、按客户种类、及/或按地理位置被指定)，并且事件管理服务器320与所述组织的所述多个闸道器310连接。应注意的是，可有多个事件管理服务器320彼此连接以交换已学习的信息。

[0107] 系统300可被设置以用于阶层的恶意代码监控，所述阶层的恶意代码监控可增进监控多个连线建立的效率，所述多个连线建立可常发生。每一用户302为连线建立而被监控。所述多个连线建立被闸道器310分析以识别所述可疑企图的子集，所述可疑企图的子集以多个可疑连线建立企图呈现。由事件管理服务器320进行所述多个可疑企图的品质保证以检测一假阳性识别。

[0108] 图3B绘示一系统350的一体系架构，于所述系统350中，所述闸道器及事件管理服务器被整合至单一元件，即一被组合的服务器354。多个用户352与所述被组合的服务器354进行通信。系统350可被设计，例如以用于一小组织，或一隔离的部门，于所述小组织或所述隔离的部门中，每一服务器354为一群组的用户352服务，提供识别所述可疑企图及进行所述可疑企图的品质保证两项功能。应注意的是，可有多个被组合的服务器354(例如，跨所述组织)可或可不彼此连接。

[0109] 系统350可被设计以用于局部恶意代码监控，而可提供快速的连线建立的监控，所述快速的连线建立的监控是例如对于地理隔离的一组织、具有有限带宽可用性的一组织，及于其中需要快速地进行连线建立的监控(例如，以减少所述连线建立的批准的时间，及/或提供高频率的连线建立)的一组织。

[0110] 现回到参照图1B及图2，闸道器210及/或服务器216可为用于安装在一计算机上的一软件模块，及/或用于与多个其它计算机通信的一硬件装置。闸道器210及/或服务器216可例如以与网络206连接的方式被安装、在一或多个用户202与网络206之间的一接口处(例如，网络接口设备)被安装，及/或被安装于网络206本身内的设备内，所述设备例如为一内部及/或边界网络设备(例如，一个二层设备、一个三层设备、一路由器、一闸道器及一桥接器)。

[0111] 经授权安装的被允许的代码208C仍可引起用于一恶意通信的连线建立的一可疑

企图的一识别，如本文所述。被允许的代码208C与流动数据相关连，所述流动数据与多个被感染的应用程序的流动数据相似及/或具有高度相关性。

[0112] 在152中，在用户处与所述连线建立过程相关的流动数据被收集，所述流动数据包括调用堆栈数据，所述收集的步骤是例如由所述用户的所述处理器可实现的终点模块208A的代码进行。所述流动数据在所述连线建立过程之前及/或中被采集。

[0113] 所述数据可包括在所述流动数据中的多笔记录，所述流动数据代表程序、多个线程及多个模块，及在所述用户端处被执行的动态代码。流动数据在所述命令引发建立所述网络连线的期间被获得，所述流动数据例如为与多个线程、多个程序及/或多个模块相关的流动数据。

[0114] 可选地，上下文数据被收集。所述上下文数据可被存储以用于之后被传输至所述品质服务器。

[0115] 可选地，在154中，多个连线建立被监控以识别建立多个网络连线的多个企图。所述监控及/或分析可在每一用户202处由个别的模块208A进行，及/或由闸道器210分别对于多个连接的用户202进行。

[0116] 可替换地或额外地，新的代码(例如，一应用程序、一插件、一修补程序、及一附加程序)的安装被例如终点模块208A识别出。所述新的代码可特意地被所述使用者安装，甚至可安全行事，但可进行违反公司策略的多个动作。例如，安装策略可禁止软件，所述软件例如是多个搭载应用程序、多个浏览器的附加程序、及多个实时通信应用程序。如此的代码可被识别为违反公司策略，例如为代表一保安威胁(例如，被用于劫持)、滥用多个有限的资源(例如，过度使用公司带宽)、及/或被公司管理决定是分散工作注意力的时间的浪费。如本文所使用，术语「恶意通信」也是指违反策略而被安装的代码的活动，不论代码本身是恶意的或安全的。与新被安装的应用程序相关的流动数据可被分析(如本文所述)，以识别建立所述连线尝试是与恶意通信相关联，所述恶意通信可代表被允许的但违背策略的行为。

[0117] 用于检测连线建立的所述多个系统及/或方法的额外细节可例如参照美国临时专利申请案号62/083,985被描述。所述美国临时专利申请案号62/083,985是由与本申请案相同的申请人及相同的多个发明人提出。

[0118] 在158中，所述流动数据及可选地所述上下文数据被从用户202传输至闸道器210，所述传输的步骤例如是由终点模块208A所进行，所述终点模块208A可存取用户202内的所述堆栈数据及/或其它流动数据。

[0119] 在160中，所述数据被分析以检测由被安装于用户202上的代码而来的建立用于一恶意活动及/或通信的一连线的一可疑企图。所述堆栈跟踪及/或其它流动数据可被分析以决定建立一恶意通信而将所述网络连线使用于恶意活动的一可疑尝试存在或不存在。可选地，所述分析的步骤是通过闸道器210可选地使用一套规则224及/或另一策略执行模块而进行。

[0120] 可选地，代表所述恶意通信存在或不存在的一信号被产生。

[0121] 所述分析的步骤可在所述应用程序与所述远程服务器或恶意服务器之间的数据通信前被进行，所述数据通信例如为由所述引发应用程序通过所述网络进行的数据前送。可选地，所述分析的步骤是在建立所述网络连线前被进行。可替换地或额外地，所述分析的步骤是在激活所述网络会话前被进行。如此，在所述恶意代理能通过所述网络连线行动前，

例如在传输未经授权的数据(即,窃取数据)前,所述连线建立过程的有效性可被决定。

[0122] 所述分析的步骤可基于一或多个方法进行,例如,使其彼此有相关性可被进行以识别与恶意活动相关联的(例如,多个堆栈跟踪、所述堆栈中的多个模块、及多个独特的事件的)一统计显着的相关性,及/或与被验证过的安全活动相关联的一统计显着的相关性。所述分析的步骤可基于核实在所述堆栈中的多个模块、多个线程及/或程序的可执行档格式的安全性被进行,例如而识别所述多笔记录为代表非法的流动数据的发生。

[0123] 多个分析方法的额外细节可例如参照美国临时专利申请案号62/083,985被找到。

[0124] 可替换地,所述闸道器的分析的步骤不果断地决定所述连线建立的企图是与恶意代码或被允许的代码相关。例如,与恶意代码相关的机率是约50%及/或与被允许的代码相关的机率是约50%。多个其它的果断决定的要求可被使用,所述多个其它的果断决定的要求例如为多个其它机率阈值、多个其它范围、及/或多个函数。如此之情况可例如在所述闸道器识别出在所述用户端上的一可疑应用程序安装程序企图引发一通信会话时发生。可选地,一消息被所述闸道器传输至所述个别的用户端,所述消息具有由一使用者(例如,操作员、系统管理员)进行手动干预的一请求,例如,一弹出窗口可在所述用户端的一显示器出现。所述使用者被提供手动定义所述代码为被允许的代码及/或恶意代码的能力,所述手动定义的步骤例如是通过点击所述弹出窗口内的一按键而进行。所述手动的指定可被加入至与所述闸道器相关联的所述一套规则,以应用在相同的用户的多个未来的通信建立企图。至多个其它闸道器的传播及/或对多个其它用户的应用可被一管理员及/或多个被预定的系统偏好设定定义。例如,对多个其它用户的应用可在(于其中仅允许有多个经注册雇员)的一私人组织网络中被启用,但在一公开网络中被禁用,以防止多个恶意的使用者欺骗所述系统及标记恶意代码为被允许的。

[0125] 如本文中所使用,词组「之前被观测的」包括手动的指定的情况。所述手动的指定被(本文所述的所述多个系统及方法)加工及/或处理,如参照词组「之前被观测的」所述。应注意的是,手动的指定在所述系统及/或方法没有进行所述之前的观测,并以将手动的指定定义为所述之前的观测取代的情况下被看待为是之前被观测的。

[0126] 可选地,在161中,当由闸道器210而来的所述分析(方框160)被决定是代表被允许的行为时,所述连线建立被允许。当没有可疑企图被检测到时,例如通过从闸道器210传输一消息至用户202,所述连线建立可恢复(及/或所述网络连线可被激活)。由品质服务器216所进行的所述一或多个堆栈跟踪的额外分析的步骤可为不必要。

[0127] 可选地,在162中,当由闸道器210而来的所述分析(方框160)被决定是代表一恶意连线的企图,所述流动数据被传输至事件管理服务器216以用于额外的分析的步骤,所述流动数据包括调用堆栈数据,所述传输的步骤例如是由闸道器210所进行。

[0128] 闸道器210(及/或用户202)可传送从用户202所取回的额外的上下文数据至服务器216,所述额外的上下文数据与所述调用堆栈数据相关联,以用于协助所述调用堆栈数据的分析的步骤,如本文所述。所述上下文数据可在方框160的所述分析的步骤指示有恶意通信企图后被收集,或可与所述流动数据一起被收集。

[0129] 可选地,闸道器210产生及传输一消息至服务器216,而请求所述可疑结果的品质保证。

[0130] 在164中,所述流动数据及可选的上下文数据被聚合及/或被分析以更正所述闸道

器的所述分析并识别所述恶意活动为正常的(即,更正一假阳性结果)。所述分析的步骤可基于聚合模块218在事件管理服务器216处被进行,如本文例如参照图1A所述。所述分析的步骤可防止或减少一假阳性识别。所述恶意结果可被重分类为正常被允许的活动。

[0131] 现参照图4A至4B,其是依据本发明的一些实施例的多个调用堆栈的多个示例,所述多个调用堆栈与所述连线建立过程相关。为清楚的目的,图4A至4B绘示一部份的跟踪。

[0132] 图4A绘示一浏览器的一调用堆栈402,所述网页浏览器具有一保安工具被安装于所述浏览器内,以提供受信任的浏览。所述保安工具通过代码的插入被实现,所述代码被设计以操纵多个HTTP会话。所述保安工具(其为一被允许的代码)与恶意代码相似地操作,且会除此以外例如在被所述闸道器分析时产生一假阳性。

[0133] 调用堆栈402代表建立一连线的一企图,例如以连接至安全的网站。调用堆栈402通过与调用堆栈404比对而被分析,所述调用堆栈404代表一验证通过的连线建立相关堆栈,所述验证通过的连线建立相关堆栈是没有所述被安装的保安工具的一网页浏览器所预期有的。所述分析的步骤检测到某个档案408(即,shlwapi.dll)为找不到,且至一已知的模块406A的一代码指针及至一未知的模块406B的另一代码指针为存在。基于(例如,由闸道器210所进行的)所述流动数据的初步分析的步骤,怀疑有恶意代码。(例如,由品质服务器216所进行的)的进一步分析的步骤基于见于被指定属于相同的组织的大多或所有其它用户的多个调用堆栈,而决定调用堆栈402代表正常代码的被允许的行为。

[0134] 图4B绘示一浏览器程序的一调用堆栈412,在所述浏览器程序中,一使用者安装了一浏览器工具栏,所述浏览器工具栏重定向及操纵多个连线,主要以影响多个搜索引擎的结果。所述工具栏非为必要地代表绝对的恶意代码,而为由一受敬重的供应商所提供的一安全的应用程序。所述工具栏被所述组织指定为被禁止安装。

[0135] 具有所述工具栏的所述浏览器企图建立一网络连线以至一已知安全的网站。堆栈412包含与所述被禁止的程序相关联的已知的代码416。相比之下,调用堆栈414为没有所述被安装的工具栏的一网页浏览器的一调用堆栈。调用堆栈414包含至一模块418(即,shlwapi.dll)的一指针,所述模块418不存在于调用堆栈416中。所述已知的调用堆栈可被编入所述学习模块,以识别具有所述被安装的工具栏的多个网页浏览器为违反公司的安装策略。

[0136] 现回到参照图1B,在166中,指示所述分析的步骤的结果的一消息被事件管理服务器216产生。所述消息被传输至闸道器210及/或用户202。所述消息可包括对所述一套规则的一更新,所述更新指示所述被匹配到的流动数据事件代表多个被允许的连线建立企图。

[0137] 当所述消息指示所述恶意通信被经不正确地检测到时,所述闸道器210及/或用户202可继续连线建立过程,及/或激活所述连线。当所述消息指示所述恶意通信被经正确地检测到时,所述闸道器210及/或用户202可阻挡(或继续维持阻挡)所述连线建立及/或防止通过所述连线进行数据传输。

[0138] 可选地,在168中,与事件管理服务器216连接的每一闸道器210的每一套规则224被以所述被接收的一套规则更新。更新每一闸道器210的所述一套规则224动态地以新的被识别的流动数据将与事件管理服务器216连接的所述多个闸道器210调适,所述新被识别的流动数据与新的被安装在多个用户202内的代码相关。

[0139] 附图中的所述流程图和所述多个框图显示了依据本发明的各种实施例的多个系

统、多个方法和多个计算机程序产品的可能实现的体系架构、功能和操作。在这方面，所述流程图或所述多个框图中的每个方框可代表一模块、一程序段或多个代码的一部分，所述模块、所述程序段或所述多个代码的所述部分包含用于实现规定的逻辑功能的一或多个可执行指令。也应注意的是，在一些替换的实现中，在所述方框中被标注的多个功能可不同于在附图中被标注的顺序发生。例如，两个被连续显示的方框实际上可实质并行地被执行，或所述两个方框有时也可按相反的顺序被执行，依照被设及的所述功能而定。也要注意的是，所述框图及/或所述流程图例证中的每个方框、及在所述框图及/或所述流程图例证中的多个方框的多个组合，能够由多个专用的基于硬件的系统来实现，所述多个专用的基于硬件的系统进行所述多个被规定的功能或动作，或多个专用硬件与计算机指令的多个组合。

[0140] 关于本发明的各种实施例的描述已经出于例证的目的而给出，但是并非意图是穷尽性的或者限定于所公开的多个实施例。在不脱离所述多个实施例的范围和精神的情况下，许多修改和变化将会是本领域技术人员所清楚的。本文所使用的术语被选择以最佳地解释所述多个实施例的原理、实际应用或者相对市场上可找得到的技术的技术改进，或者使得本领域技术人员能够理解本文所公开的多个实施例。

[0141] 可预期的是，从本申请的成熟而来的一专利的生命期间，许多有关的多个系统及方法将被开发，且多个术语「用户」、「服务器」、及「代码」的范围意图是以先验包含所有如此之新的技术。

[0142] 如本文所用的术语“约”是指±10％。

[0143] 多个术语「包含(comprises)」、「包含(comprising)」、「包括(includes)」、「包括(including)」、「具有(having)」及其多个词形变化是指「包括但不限于」。此术语包含多个术语「由.....组成(consisting of)」及「基本上由.....组成(essentially consisting of)」。

[0144] 术语「基本上由.....组成(essentially consisting of)」是指组合物或方法可包括多个额外的成分及/或多个步骤，但只有当所述多个额外的成分及/或多个步骤实质上不改变所要求保护的组合物或方法的多个基本特征及新特征。

[0145] 本文所使用的单数型式「一」、「一个」及「所述」包括复数引用，除非上下文另有明确规定。例如，术语「一化合物」或「至少一种化合物」可以包括多个化合物，包括其混合物。

[0146] 本文中所用的词汇「示例性(exemplary)」表示「用作为一示例(example)，实例(instance)或例证(illustration)」。任何被描述为「示例性」实施例未必被解释为优选或优于其它实施例和/或排除与来自其它实施例的多个特征结合。

[0147] 本文中所用的词汇「可选择地(optionally)」表示「在一些实施例中提供，而在多个其它实施例中不提供」。任何本发明的特定实施例可以包括多个「可选择的」特征，除非此类特征相冲突。

[0148] 在整个本申请中，本发明的各种实施例可以以一个范围的形式存在。应当理解，以一范围形式的描述仅仅是因为方便及简洁，不应理解为对本发明范围的硬性限制。因此，应当认为所述的范围描述已经具体公开所有可能的子范围以及该范围内的多个单一数值。例如，应当认为从1到6的范围描述已经具体公开子范围，例如从1到3，从1到4，从1到5，从2到4，从2到6，从3到6等，以及所数范围内的多个单一数字，例如1、2、3、4、5及6，此不管范围为何皆适用。

[0149] 每当在本文中指出一数值范围，是指包括所指范围内的任何引用的数字(分数或整数)。术语，第一指示数字及第二指示数字「之间的范围」及第一指示数字「到」第二指示数字「的范围」在本文中可互换，并指包括第一及第二指示数字，及其间的所有分数及整数。

[0150] 可以理解，本发明中的某些特征，为清楚起见，在分开的实施例的内文中描述，也可以在单一实施例的组合中提供。相反地，本发明中，为简洁起见，在单一实施例的内文中所描述的各种特征，也可以分开地、或者以任何合适的子组合、或者在适用于本发明的任何其它描述的实施例中提供。在各种实施例的内文中所描述的某些特征，并不被认为是那些实施方案的必要特征，除非该实施例没有那些元素就不起作用。

[0151] 虽然本发明结合其具体实施例而被描述，显而易见的是，许多替换、修改及变化对于那些本领域的技术人员将是显而易见的。因此，其意图在包括落入所附权利要求书的范围内的所有替换、修改及变化。

[0152] 在本说明书中提及的所有出版物、专利及专利申请以其整体在此通过引用并入本说明书中。其程度如同各单独的出版物、专利或专利申请被具体及单独地指明而通过引用并入本文中。此外，所引用的或指出的任何参考文献不应被解释为承认这些参考文献可作为本发明的现有技术。本申请中标题部分在本文中用于使本说明书容易理解，而不应被解释为必要的限制。

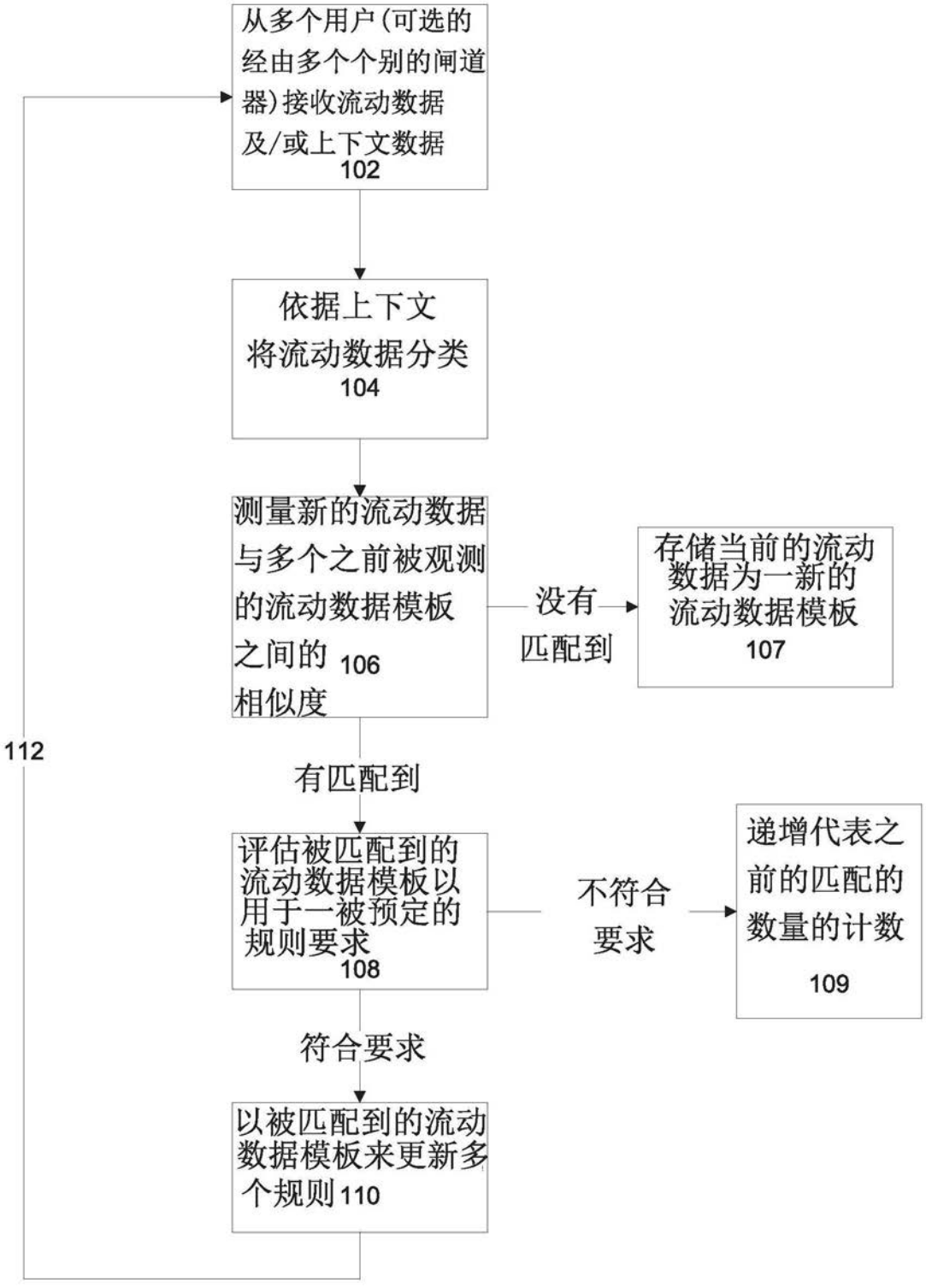

从多个用户(可选的经由多个个别的闸道器)接收流动数据及/或上下文数据
102
依据上下文将流动数据分类
104
测量新的流动数据与多个之前被观测的流动数据模板之间的相似度
106
没有匹配到
存储当前的流动数据为一新的流动数据模板
107
有匹配到
评估被匹配到的流动数据模板以用于一被预定的规则要求
108
不符合要求
递增代表之前的匹配的数量的计数
109
符合要求
以被匹配到的流动数据模板来更新多个规则
110
112

图1A

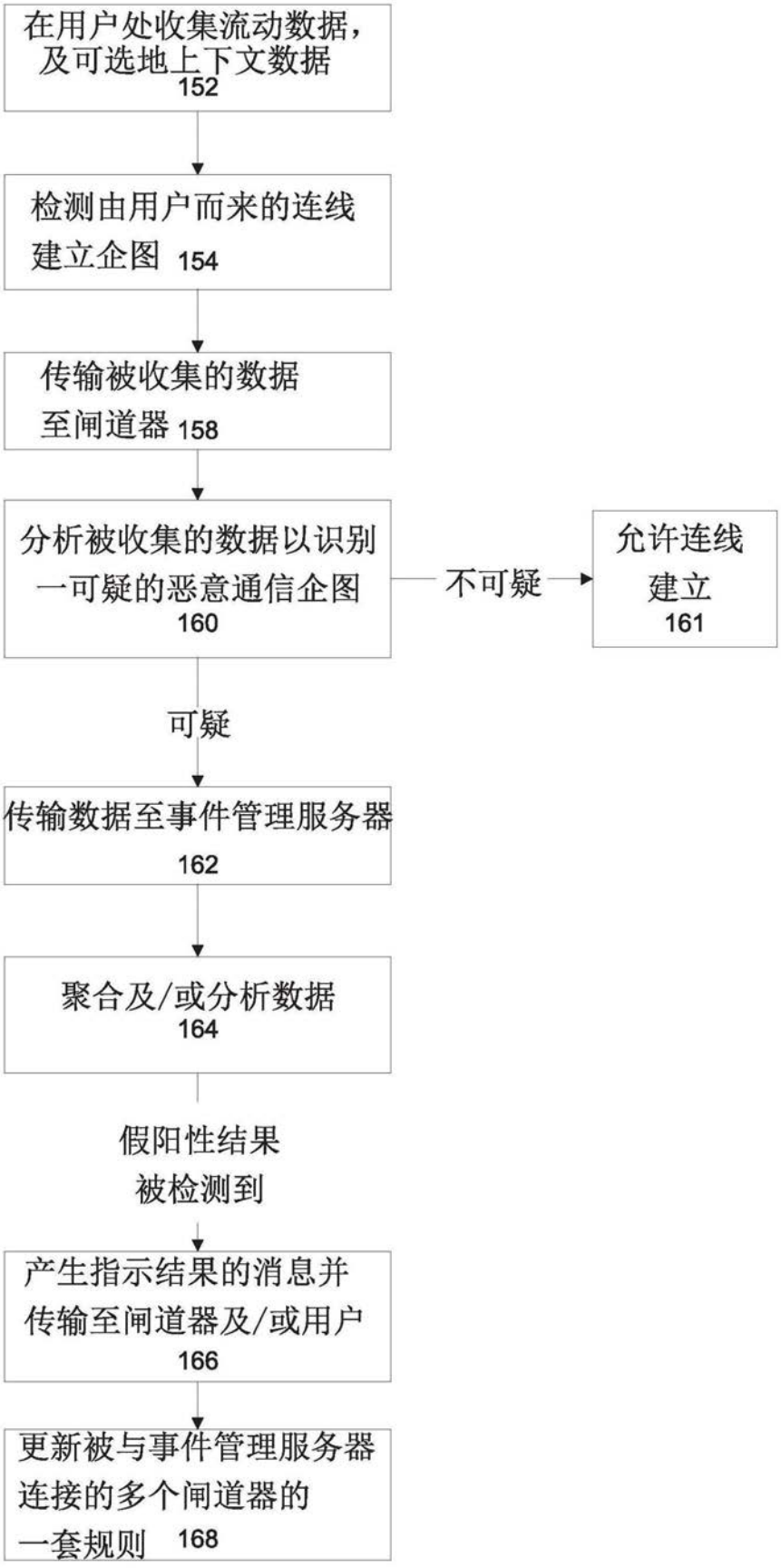

在用户处收集流动数据，及可选地上下文数据 152
检测由用户而来的连线建立企图 154
传输被收集的数据至闸道器 158
分析被收集的数据以识别一可疑的恶意通信企图 160
不可疑
允许连线建立 161
可疑
传输数据至事件管理服务器 162
聚合及/或分析数据 164
假阳性结果被检测到
产生指示结果的消息并传输至闸道器及/或用户 166
更新被与事件管理服务器连接的多个闸道器的一套规则 168

图1B

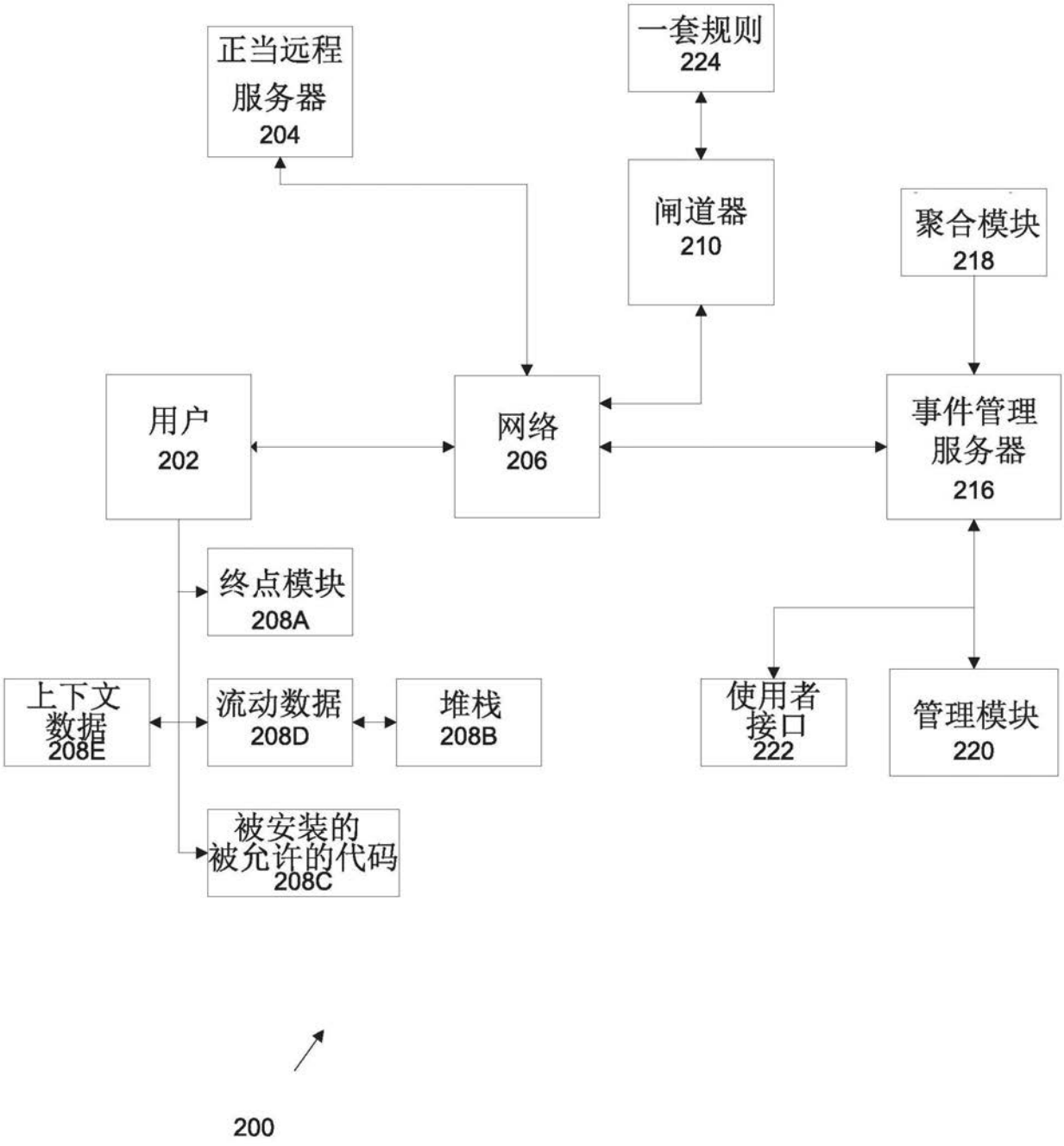

正当远程
服务器
204
一套规则
224
闸道器
210
聚合模块
218
用户
202
网络
206
事件管理
服务器
216
终点模块
208A
上下文
数据
208E
流动数据
208D
堆栈
208B
使用者
接口
222
管理模块
220
被安装的
被允许的代码
208C
200

图2

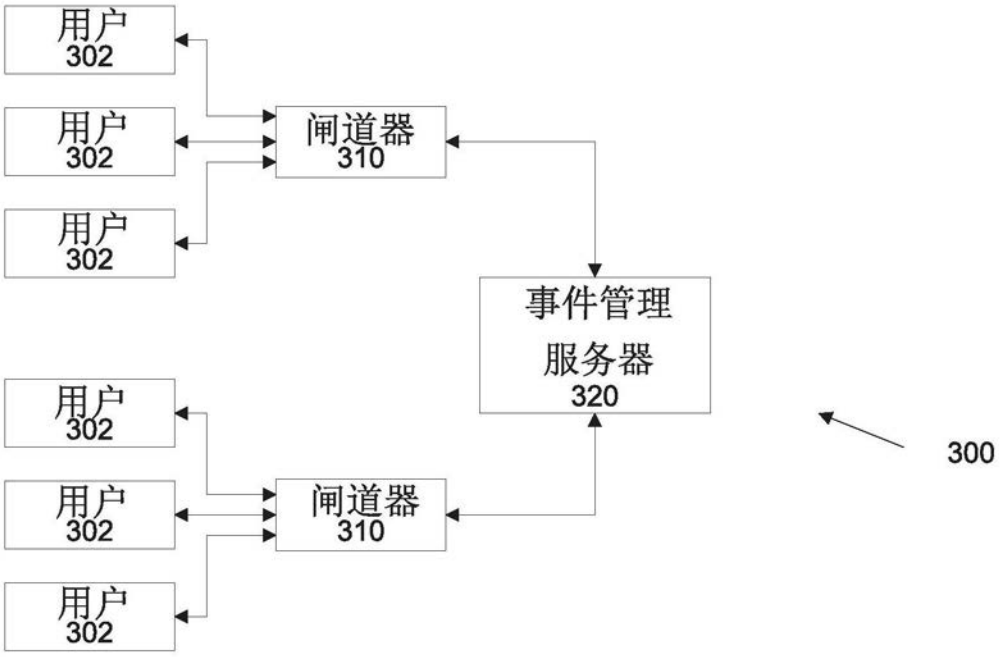

用户
302
用户
302
用户
302
闸道器
310
事件管理
服务器
320
用户
302
用户
302
用户
302
闸道器
310
300

图3A

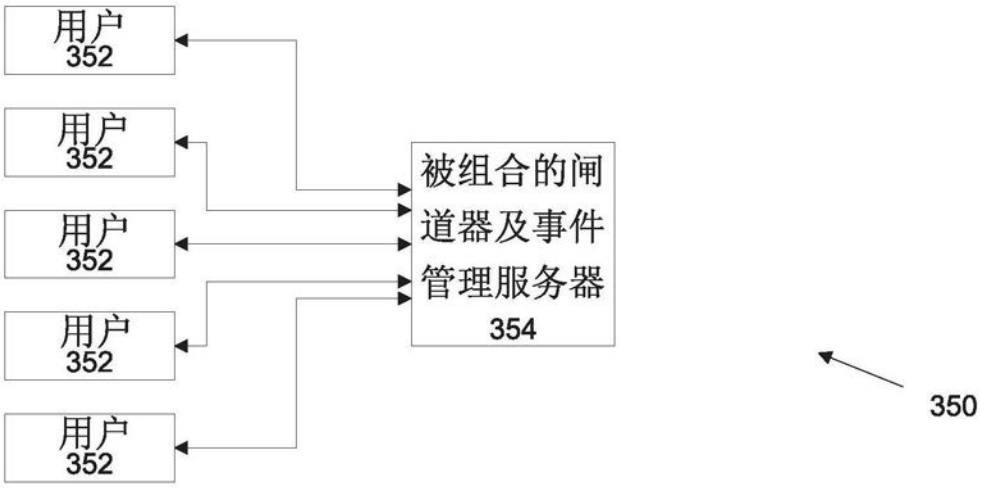

用户
352
用户
352
用户
352
用户
352
用户
352
被组合的闸
道器及事件
管理服务器
354
350

图3B

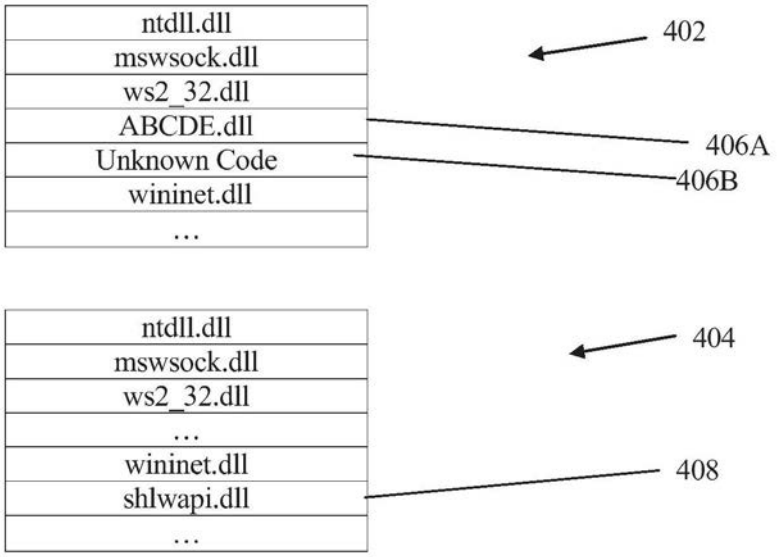

ntdll.dll
mswsock.dll
ws2_32.dll
ABCDE.dll
Unknown Code
wininet.dll
…
402
406A
406B
ntdll.dll
mswsock.dll
ws2_32.dll
…
wininet.dll
shlwapi.dll
…
404
408

图4A

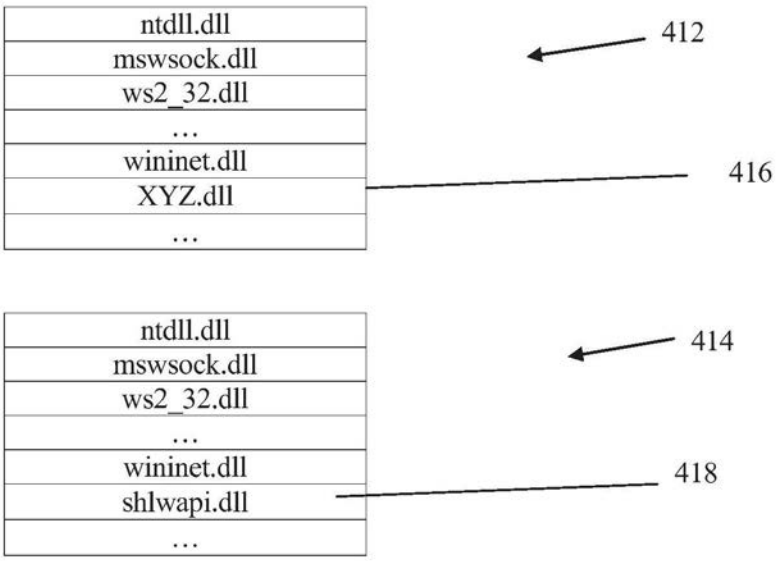

ntdll.dll
mswsock.dll
ws2_32.dll
…
wininet.dll
XYZ.dll
…
412
416
ntdll.dll
mswsock.dll
ws2_32.dll
…
wininet.dll
shlwapi.dll
…
414
418

图4B