(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 102484640 B
(45)授权公告日 2015.09.16

(21)申请号 201080038051.3
(22)申请日 2010.08.23
(30)优先权数据
2675664 2009.08.28 CA
(85)PCT国际申请进入国家阶段日
2012.02.27
(86)PCT国际申请的申请数据
PCT/EP2010/062273 2010.08.23
(87)PCT国际申请的公布数据
WO2011/023664 EN 2011.03.03
(73)专利权人 国际商业机器公司
地址 美国纽约
(72)发明人 A·H·沃尔德曼 J·考迪斯
(74)专利代理机构 北京市中咨律师事务所 11247
代理人 张亚非 于静
(51)Int.Cl.
H04L 29/06(2006.01)
(56)对比文件
CN 101193103 A,2008.06.04, 全文.
US 2007/0271379 A1,2007.11.22, 全文.
审查员 闫洪波

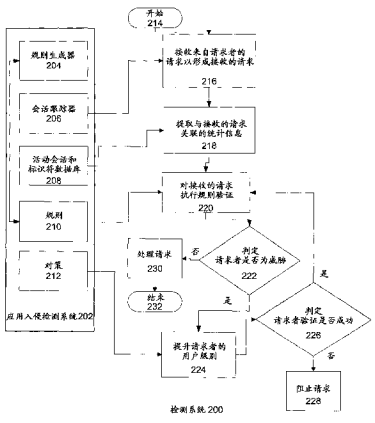
权利要求书4页 说明书10页 附图6页

(54)发明名称

用于解决检测到的威胁的方法和装置

(57)摘要

说明性实施例提供了用于解决检测到的威胁的方法。所述方法接收来自请求者的请求以形成收到的请求，提取与所述收到的请求关联的统计信息以形成提取的统计信息，使用所述提取的统计信息对所述收到的请求执行规则验证，以及判定所述请求是否为威胁。响应于判定所述请求为威胁，使用提升增量提升所述请求者的级别，其中所述使用提升增量进一步包括通过渗入到下一用户级别和直接进入一个用户级别之一来增加用户身份和验证要求。



CN 102484640 B

1. 一种用于解决检测到的威胁的方法，所述方法包括：

接收来自请求者的请求以形成收到的请求；

提取与所述收到的请求关联的统计信息以形成提取的统计信息；

使用所述提取的统计信息对所述收到的请求执行规则验证；

判定所述请求是否为威胁；以及

响应于判定所述请求为威胁，使用提升增量提升所述请求者的级别，其中所述使用提升增量包括通过渗入到下一用户级别和直接进入一个用户级别之一来增加用户身份和验证要求。

2. 如权利要求 1 中所述的方法，其中提取与所述收到的请求关联的统计信息进一步包括：

跟踪会话信息以形成跟踪的会话信息；以及

将所述跟踪的会话信息存储在活动会话和标识符数据库中。

3. 如权利要求 1 或权利要求 2 中所述的方法，其中执行规则验证进一步包括：

选择与提升增量关联的规则以形成选定规则；以及

将所述选定规则应用于所述收到的请求。

4. 如权利要求 2 中所述的方法，其中判定所述请求是否为威胁进一步包括：

将所述跟踪的会话信息与和提升增量的用户级别关联的预定标准进行比较以形成比较；以及

判定所述比较是否超过预定阈值。

5. 如权利要求 1、2 和 4 中任一权利要求中所述的方法，其中所述使用提升增量提升所述请求者的级别进一步包括：

判定所述请求是否为威胁；

响应于判定所述请求为威胁，提示所述请求者进行验证；

判定是否使用实时代理；

响应于判定使用实时代理，与所述实时代理对话；

判定所述验证是否成功；以及

响应于判定所述验证未成功，阻止所述请求。

6. 如权利要求 3 中所述的方法，其中，所述使用提升增量提升所述请求者的级别进一步包括：

判定所述请求是否为威胁；

响应于判定所述请求为威胁，提示所述请求者进行验证；

判定是否使用实时代理；

响应于判定使用实时代理，与所述实时代理对话；

判定所述验证是否成功；以及

响应于判定所述验证未成功，阻止所述请求。

7. 如权利要求 5 中所述的方法，其中响应于判定未使用所述实时代理：

提示所述请求者提供所需的信息；

判定所述验证是否成功；

响应于判定所述验证成功，重新评估所述请求。

8. 如权利要求 6 中所述的方法，其中响应于判定未使用所述实时代理：

提示所述请求者提供所需的信息；

判定所述验证是否成功；

响应于判定所述验证成功，重新评估所述请求。

9. 如权利要求 1、2 和 4 中任一权利要求中所述的方法，其中使用提升增量提升所述请求者的级别进一步包括：

使用选定的一个提升增量创建提升请求；

判定所述提升请求是否成功；以及

响应于判定所述提升请求成功，重新评估所述请求；以及

响应于判定所述提升请求未成功，阻止所述请求。

10. 如权利要求 3 中所述的方法，其中使用提升增量提升所述请求者的级别进一步包括：

使用选定的一个提升增量创建提升请求；

判定所述提升请求是否成功；以及

响应于判定所述提升请求成功，重新评估所述请求；以及

响应于判定所述提升请求未成功，阻止所述请求。

11. 如权利要求 5 中所述的方法，其中使用提升增量提升所述请求者的级别进一步包括：

使用选定的一个提升增量创建提升请求；

判定所述提升请求是否成功；以及

响应于判定所述提升请求成功，重新评估所述请求；以及

响应于判定所述提升请求未成功，阻止所述请求。

12. 如上述权利要求 6 中所述的方法，其中使用提升增量提升所述请求者的级别进一步包括：

使用选定的一个提升增量创建提升请求；

判定所述提升请求是否成功；以及

响应于判定所述提升请求成功，重新评估所述请求；以及

响应于判定所述提升请求未成功，阻止所述请求。

13. 如上述权利要求 7 中所述的方法，其中使用提升增量提升所述请求者的级别进一步包括：

使用选定的一个提升增量创建提升请求；

判定所述提升请求是否成功；以及

响应于判定所述提升请求成功，重新评估所述请求；以及

响应于判定所述提升请求未成功，阻止所述请求。

14. 如上述权利要求 8 中所述的方法，其中使用提升增量提升所述请求者的级别进一步包括：

使用选定的一个提升增量创建提升请求；

判定所述提升请求是否成功；以及

响应于判定所述提升请求成功，重新评估所述请求；以及

响应于判定所述提升请求未成功，阻止所述请求。

15. 一种用于解决检测到的威胁的装置，所述装置包括：

用于接收来自请求者的请求以形成收到的请求的装置；

用于提取与所述收到的请求关联的统计信息以形成提取的统计信息的装置；

用于使用所述提取的统计信息对所述收到的请求执行规则验证的装置；

用于判定所述请求是否为威胁的装置；以及

用于响应于判定所述请求为威胁，通过渗入到下一用户级别和直接进入一个用户级别之一来增加用户身份和验证要求，使用提升增量提升所述请求者的级别的装置。

16. 如权利要求 15 中所述的装置，其中所述提取装置进一步包括：

用于跟踪会话信息以形成跟踪的会话信息的装置；以及

用于将所述跟踪的会话信息存储在活动会话和标识符数据库中的装置。

17. 如权利要求 15 或权利要求 16 中所述的装置，其中所述用于使用所述提取的统计信息对所述收到的请求执行规则验证的装置进一步包括：

用于选择与提升增量关联的规则以形成选定规则的装置；以及

用于将所述选定规则应用于所述收到的请求的装置。

18. 如权利要求 16 中所述的装置，其中所述判定装置进一步包括：

用于将所述跟踪的会话信息与和提升增量的用户级别关联的预定标准进行比较以形成比较的装置；以及

用于判定所述比较是否超过预定阈值的装置。

19. 如权利要求 15、16 和 18 中任一权利要求中所述的装置，其中所述使用提升增量提升所述请求者的级别的装置进一步包括：

用于判定所述请求是否为威胁的装置；

用于响应于判定所述请求为威胁，提示所述请求者进行验证的装置；

用于判定是否使用实时代理的装置；

用于响应于判定使用实时代理，与所述实时代理对话的装置；

用于判定所述验证是否成功的装置；

用于响应于判定所述验证未成功，阻止所述请求的装置。

20. 如权利要求 17 中所述的装置，其中所述使用提升增量提升所述请求者的级别的装置进一步包括：

用于判定所述请求是否为威胁的装置；

用于响应于判定所述请求为威胁，提示所述请求者进行验证的装置；

用于判定是否使用实时代理的装置；

用于响应于判定使用实时代理，与所述实时代理对话的装置；

用于判定所述验证是否成功的装置；

用于响应于判定所述验证未成功，阻止所述请求的装置。

21. 如权利要求 19 中所述的装置，进一步包括，响应于判定未使用所述实时代理：

用于提示所述请求者提供所需的信息的装置；

用于判定所述验证是否成功的装置；以及

用于响应于判定所述验证成功，重新评估所述请求的装置。

22. 如权利要求 20 中所述的装置，进一步包括，响应于判定未使用所述实时代理：

用于提示所述请求者提供所需的信息的装置；

用于判定所述验证是否成功的装置；以及

用于响应于判定所述验证成功，重新评估所述请求的装置。

23. 如权利要求 15、16 和 18 中任一权利要求中所述的装置，其中所述使用提升增量提升所述请求者的级别的装置进一步包括：

用于使用选定的一个提升增量创建提升请求的装置；

用于判定所述提升请求是否成功的装置；以及

用于响应于判定所述提升请求成功，重新评估所述请求的装置；以及

用于响应于判定所述提升请求未成功，阻止所述请求的装置。

24. 如权利要求 17 中所述的装置，其中所述提升装置进一步包括：

用于使用选定的一个提升增量创建提升请求的装置；

用于判定所述提升请求是否成功的装置；以及

用于响应于判定所述提升请求成功，重新评估所述请求的装置；以及

用于响应于判定所述提升请求未成功，阻止所述请求的装置。

25. 如权利要求 19 中所述的装置，其中所述使用提升增量提升所述请求者的级别的装置进一步包括：

用于使用选定的一个提升增量创建提升请求的装置；

用于判定所述提升请求是否成功的装置；以及

用于响应于判定所述提升请求成功，重新评估所述请求的装置；以及

用于响应于判定所述提升请求未成功，阻止所述请求的装置。

26. 如权利要求 20 中所述的装置，其中所述使用提升增量提升所述请求者的级别的装置进一步包括：

用于使用选定的一个提升增量创建提升请求的装置；

用于判定所述提升请求是否成功的装置；以及

用于响应于判定所述提升请求成功，重新评估所述请求的装置；以及

用于响应于判定所述提升请求未成功，阻止所述请求的装置。

27. 如权利要求 21 中所述的装置，其中所述使用提升增量提升所述请求者的级别的装置进一步包括：

用于使用选定的一个提升增量创建提升请求的装置；

用于判定所述提升请求是否成功的装置；以及

用于响应于判定所述提升请求成功，重新评估所述请求的装置；以及

用于响应于判定所述提升请求未成功，阻止所述请求的装置。

28. 如权利要求 22 中所述的装置，其中所述使用提升增量提升所述请求者的级别的装置进一步包括：

用于使用选定的一个提升增量创建提升请求的装置；

用于判定所述提升请求是否成功的装置；以及

用于响应于判定所述提升请求成功，重新评估所述请求的装置；以及

用于响应于判定所述提升请求未成功，阻止所述请求的装置。

用于解决检测到的威胁的方法和装置

技术领域

[0001] 本发明一般地涉及数据处理系统中的威胁检测。

背景技术

[0002] web 应用可能会遭受有意或无意的滥用和攻击。诸如拒绝服务(DoS)、蛮力攻击(brute force)或利用无边界条件(unbounded condition)之类的应用层攻击通过限制应用的可用性和完整性来影响企业。确定问题并部署解决方案可能会非常耗时。当问题存在时,应用会继续不可用,通常导致收益损失。替代地,限制对应用的访问是无效的,因为攻击代理可以轻松地更改位置,并且置于网络层的任何障碍都可能对应用的有效用户社区产生巨大影响。

[0003] 一般的解决方案会在发生可疑活动时瞄准网络层。但是,如上所述,应用层攻击经常是无意的。经常地,实施异常但非恶意行为的网络蜘蛛程序(web crawler)(也称为机器人或简称为bot)、业务伙伴或用户会造成应用层攻击。了解有关攻击者的更多信息(攻击者经常愿意披露此类数据)会在问题解决中起到非常重要的作用。

发明内容

[0004] 根据一个实施例,提供了一种计算机实现的用于解决检测到的威胁的方法。所述计算机实现的过程接收来自请求者的请求以形成收到的请求,提取与所述收到的请求关联的统计信息以形成提取的统计信息,使用所述提取的统计信息对所述收到的请求执行规则验证,以及判定所述请求者是否为威胁。响应于判定所述请求者为威胁,使用提升增量提升所述请求者的级别,其中所述使用提升增量进一步包括通过渗入到下一用户级别或直接进入一个用户级别之一来增加用户身份和验证要求。

[0005] 根据另一实施例,提供了一种用于解决检测到的威胁的计算机程序产品,所述计算机程序产品包括包含上面存储的计算机可执行程序代码的计算机可记录介质,所述计算机可执行程序代码包括用于接收来自请求者的请求以形成收到的请求的计算机可执行程序代码,用于提取与所述收到的请求关联的统计信息以形成提取的统计信息的计算机可执行程序代码,用于使用所述提取的统计信息对所述收到的请求执行规则验证的计算机可执行程序代码,用于判定所述请求是否为威胁的计算机可执行程序代码,以及用于响应于判定所述请求为威胁,使用提升增量提升所述请求者的级别的计算机可执行程序代码,其中所述用于使用提升增量的计算机可执行程序代码进一步包括用于通过渗入(percolate)到下一用户级别或直接进入一个用户级别之一来增加用户身份和验证要求的计算机可执行程序代码。

[0006] 根据另一实施例,提供了一种用于解决检测到的威胁的装置。所述装置包括通信结构、与所述通信结构相连的存储器(其中所述存储器包含计算机可执行程序代码)、与所述通信结构相连的通信单元、与所述通信结构相连的输入/输出单元、与所述通信结构相连的显示器以及与所述通信结构相连的处理器单元,其中所述处理器单元执行所述计算机

可执行程序代码以引导所述装置接收来自请求者的请求以形成收到的请求，提取与所述收到的请求关联的统计信息以形成提取的统计信息，使用所述提取的统计信息对所述收到的请求执行规则验证，判定所述请求是否为威胁，以及响应于判定所述请求为威胁，使用提升增量提升所述请求者的级别，其中所述使用提升增量进一步包括通过渗入到下一用户级别或直接进入一个用户级别之一来增加用户身份和验证要求。

附图说明

[0007] 为了更全面地理解本发明，现在结合附图，参考下面的简要描述以及详细的描述，其中相同的标号表示相同的部分。

[0008] 图 1 是可针对本发明的各实施例运行的示例性数据处理系统的方块图；

[0009] 图 2 是根据本发明的各实施例的基于异常的应用入侵检测系统的流程图；

[0010] 图 3 是根据本发明的一个实施例与图 2 中的基于异常的应用入侵检测系统结合使用的提升增量和用户级别的方块图；

[0011] 图 4 是根据本发明的一个实施例使用图 3 中的用户级别的阻止过程的流程图；

[0012] 图 5a 是根据本发明的一个实施例的图 4 中的提升过程的流程图；以及

[0013] 图 5b 是根据本发明的一个实施例的图 5a 中的验证过程的流程图。

具体实施方式

[0014] 尽管下面提供了一个或多个实施例的说明性实现，但是所披露的系统和 / 或方法可以使用任意多种技术来实现。本发明绝不限于下面展示的说明性的实现、附图和技术，包括在此示出和描述的示例性设计和实现，而是可以在所附权利要求及其等价物的全部范围内进行修改。

[0015] 本领域的技术人员将理解，本发明可以实现为系统、方法或计算机程序产品。因此，本发明可以采取完全硬件实施例、完全软件实施例（包括固件、驻留软件、微代码等）或组合了软件和硬件方面的实施例的形式，所有这些方面在此通常被称为“电路”、“模块”或“系统”。此外，本发明可以采取有形地体现在任何表现介质（在介质中具有计算机可用程序代码）中的计算机程序产品的形式。

[0016] 用于执行本发明的操作的计算机程序代码可以使用一种或多种编程语言的任意组合来编写，所述编程语言包括诸如 Java™、Smalltalk、C++ 或类似语言之类的面向对象的编程语言以及诸如“C”编程语言或类似的编程语言之类的常规过程编程语言。Java 和所有基于 Java 的商标和徽标是 Sun Microsystems, 公司在美国和 / 或其他国家 / 地区的商标。所述程序代码可以完全地在用户计算机上执行，部分地在用户计算机上执行，作为独立的软件包执行，部分地在用户计算机上并部分地在远程计算机上执行，或者完全地在远程计算机或服务器上执行。在后者的情况中，所述远程计算机可以通过包括局域网（LAN）或广域网（WAN）的任何类型网络与用户的计算机相连，也可以与外部计算机进行连接（例如，使用因特网服务提供商通过因特网连接）。

[0017] 下面参考根据本发明的示例性实施例的方法、装置、系统和计算机程序产品的流程图和 / 或方块图对本发明进行描述。将理解，所述流程图和 / 或方块图的每个方块以及所述流程图和 / 或方块图中的方块的组合可以由计算机程序指令来实现。

[0018] 这些计算机程序指令可以被提供给通用计算机、专用计算机或其他可编程数据处理装置的处理器以产生机器，以便通过所述计算机或其他可编程数据处理装置的处理器执行的所述指令产生用于实现在一个或多个流程图和/或方块图方块中指定的功能/操作的装置。这些计算机程序指令也可以被存储在引导计算机或其他可编程数据处理装置以特定方式执行功能的计算机可读介质中，以便存储在所述计算机可读介质中的所述指令产生一件包括实现在所述一个或多个流程图和/或方块图方块中指定的功能/操作的指令装置的制品。

[0019] 所述计算机程序指令还可被加载到计算机或其他可编程数据处理装置，以导致在所述计算机或其他可编程装置上执行一系列操作步骤以产生计算机实现的过程，从而在所述计算机或其他可编程装置上执行的指令提供用于实现在一个或多个流程图和/或方块图方块中指定的功能/操作的过程。

[0020] 现在参考图 1，其示出可针对本发明的各实施例运行的示例性数据处理系统的方块图。在该所示的示例中，数据处理系统 100 包括通信结构 102，所述通信结构提供处理器单元 104、存储器 106、持久性存储装置 108、通信单元 110、输入/输出(I/O)单元 112 和显示器 114 之间的通信。

[0021] 处理器单元 104 用于执行可以加载到存储器 106 内的软件的指令。处理器单元 104 可以是一个或多个处理器的组，也可以是多处理器核，这取决于特定的实现。进一步地，处理器单元 104 可以使用一个或多个异构处理器系统来实现，在所述异构处理器系统中，单个芯片上同时包括主处理器和从处理器。作为另一说明性示例，处理器单元 104 可以是包含多个同类型处理器的对称多处理器系统。

[0022] 存储器 106 和持久性存储装置 108 是存储设备 116 的示例。存储设备是能够存储信息的任何硬件，所述信息例如为但不限于数据、功能形式的程序代码和/或其他适当的临时和/或持久信息。在这些示例中，存储器 106 可以例如是随机存取存储器或其他任何适当的易失性或非易失性存储设备。持久性存储装置 108 可以根据特定的实现采取各种形式。例如，持久性存储装置 108 可以包含一个或多个组件或设备。例如，持久性存储装置 108 可以是硬盘驱动器、闪存、可擦写光盘、可擦写磁带或上述元件的某种组合。持久性存储装置 108 所使用的介质也可以是可拆装的。例如，可以将可拆装硬盘驱动器用作持久性存储装置 108。

[0023] 在这些示例中，通信单元 110 提供与其他数据处理系统或设备的通信。在这些示例中，通信单元 110 为网络接口卡。通信单元 110 可以通过使用物理通信链路和无线通信链路中的任何一个或两者提供通信。

[0024] 输入/输出单元 112 允许与数据处理系统 100 上连接的其他设备进行数据输入和输出。例如，输入/输出单元 112 可以提供连接，用于通过键盘、鼠标和/或其他某种适当的输入设备进行的用户输入。进一步地，输入/输出单元 112 可以将输出发送到打印机。显示器 114 提供向用户显示信息的装置。

[0025] 操作系统、应用和/或程序的指令可以位于通过通信结构 102 与处理器单元 104 通信的存储设备 116 中。在这些说明性示例中，所述指令采取位于持久性存储装置 108 中的功能形式。这些指令可以加载到存储器 106 内以便由处理器单元 104 执行。处理器单元 104 可以使用计算机实现的指令执行不同实施例的过程，所述指令可以位于诸如存储器

106 之类的存储器中。

[0026] 这些指令被称为程序代码、计算机可用程序代码或计算机可读程序代码，其可由处理器单元 104 中的处理器读取和执行。不同实施例中的程序代码可以体现于不同的物理或有形可读介质，例如存储器 106 或持久性存储装置 108 中。

[0027] 程序代码 118 采取功能形式并位于可选择性地拆装的计算机可读介质 120 中，并且可以加载或传输到数据处理系统 100 内以便由处理器单元 104 执行。在这些示例中，程序代码 118 和计算机可读介质 120 构成计算机程序产品 122。在一个示例中，计算机可读介质 120 可以采取有形形式，例如光盘或磁带，所述光盘或磁带被插入或放入作为持久性存储装置 108 的一部分的驱动器或其他设备，以便传输到诸如作为持久性存储装置 108 的一部分的硬盘的存储设备上。在有形形式中，计算机可读介质 120 还可以采取持久性存储装置的形式，所述持久性存储装置例如为与数据处理系统 100 相连的硬盘、闪盘（thumb drive）或闪存。计算机可读介质 120 的有形形式还被称为计算机可记录存储介质。在某些示例中，计算机可读介质 120 可以是不可拆装的。

[0028] 替代地，程序代码 118 可以通过与通信单元 110 的通信链路和 / 或通过与输入 / 输出单元 112 的连接从计算机可读介质 120 传输到数据处理系统 100。在所示的示例中，所述通信链路和 / 或连接可以是物理的或无线的。所述计算机可读介质还可以采取非有形介质的形式，例如通信链路或包含程序代码的无线传输。

[0029] 在某些示例性实施例中，程序代码 118 可以通过网络从另一设备或数据处理系统下载到持久性存储装置 108 中以便在数据处理系统 100 内使用。例如，服务器数据处理系统内的计算机可读存储介质中存储的程序代码可以通过网络从服务器下载到数据处理系统 100 中。提供程序代码 118 的数据处理系统可以是服务器计算机、客户端计算机或其他某种能够存储和传输程序代码 118 的设备。

[0030] 针对数据处理系统 100 示出的不同组件并非旨在对不同实施例的实现方式做出体系结构方面的限制。可以在包括作为针对数据处理系统 100 所示的那些组件的补充或替代的组件的数据处理系统中实现其他说明性实施例。图 1 中所示的其他组件可以不同于所示的说明性示例。可以使用能够执行程序代码的任何硬件设备或系统实现不同实施例。作为一个示例，数据处理系统可以包括与无机组件集成的有机组件和 / 或可以完全由不包括人类的有机组件构成。例如，存储设备可以由有机半导体组成。

[0031] 作为另一示例，数据处理系统 100 中的存储设备可以是任何可以存储数据的硬件装置。存储器 106、持久性存储装置 108 和计算机可读介质 120 是采取有形形式的存储设备的示例。

[0032] 在另一示例中，可以使用总线系统来实现通信结构 102，并且所述总线系统可以包括诸如系统总线或输入 / 输出总线之类的一条或多条总线。当然，所述总线系统可以使用在与所述总线系统相连的不同组件或设备之间提供数据传输的任何适当类型的体系结构来实现。此外，通信单元可以包括一个或多个用于发送和接收数据的设备，例如调制解调器或网络适配器。进一步地，存储器可以是例如可以在通信结构 102 中出现的接口或存储控制集线器中找到的存储器 106 或高速缓冲存储器。

[0033] 根据一个说明性实施例，提供了计算机实现的用于解决检测到的威胁的过程。所述计算机实现的过程接收来自请求者的请求以形成收到的请求，提取与所述收到的请求关

联的统计信息以形成提取的统计信息，使用所述提取的统计信息对所述收到的请求执行规则验证，以及判定所述请求者是否为威胁。响应于判定所述请求者为威胁，使用提升增量提升所述请求者的级别，其中所述提升进一步包括渗入到下一用户级别和直接进入一个用户级别。

[0034] 使用图 1 中的数据处理系统 100 作为示例，说明实施例提供了存储在存储器 106 中由处理器单元 104 执行的计算机实现的过程，所述过程，例如通过通信单元 110 或输入 / 输出单元 112，接收来自请求者的请求以形成收到的请求。处理器单元 104 提取与所述收到的请求关联的统计信息以形成可以存储在存储设备 116 中的提取的统计信息。处理器单元 104 使用所述提取的统计信息对所述收到的请求执行规则验证，以及判定所述请求者是否为威胁。响应于判定所述请求者为威胁，处理器单元 104 使用可以存储在存储器 106 或持久性存储装置 108 中的提升增量提升所述请求者，其中所述提升进一步包括渗入到下一用户级别和直接进入一个用户级别。所述提升一般涉及增加用户身份和验证要求。

[0035] 在备选实施例中，包含计算机实现的过程的程序代码 118 可以存储在计算机可读介质 120 内作为计算机程序产品 122。在另一说明性实施例中，可以在装置中实现用于通过使用分级权重的信任断言（trust assertion）进行访问控制的过程，所述装置包括通信结构、与所述通信结构相连的存储器（其中所述存储器包含计算机可执行程序代码）、与所述通信结构相连的通信单元、与所述通信结构相连的输入 / 输出单元、与所述通信结构相连的显示器以及与所述通信结构相连的处理器单元。所述装置的处理器单元执行所述计算机可执行程序代码以引导所述装置执行所述过程。

[0036] 现在参考图 2，其示出根据本发明的各种实施例的基于异常的应用入侵检测系统的流程图。检测系统 200 是能够逐步提升用户级别的基于异常的应用入侵检测系统示例。检测系统 200 可以基于新的或现有的基于异常的应用层入侵检测系统，例如基于异常的应用入侵检测系统 202。

[0037] 一般的基于异常的应用入侵检测系统（APIDS）可以由基于异常的应用入侵检测系统 202 来代表。例如，基于异常的应用入侵检测系统 202 包括若干组件，其中包括规则生成器 204、会话跟踪器 206、活动会话和标识符数据库 208、规则 210 和对策 212。

[0038] 规则生成器 204 是使用所获取的不同格式的信息来定义可变的使用基准并产生规则的组件，所述信息包括人工输入、使用历史、预测及使用异常。规则用于建立符合性标准，根据此标准，可以在开始于操作 214 的过程中度量有关接收来自请求者的请求以形成收到的请求 216 的请求。例如，当使用网站时，规则生成器 204 可以包括但不限于用于与页面分发、响应时间、每会话命中数以及上一页和下一页相关的标准的能力。

[0039] 会话跟踪器 206 是能够跟踪用户与系统的交互的组件。该组件一般包括安全会话标识机制，例如，用于与接收来自请求者的请求以形成收到的请求 216 关联的 web 应用的加密 cookie。

[0040] 活动会话和标识符数据库 208 是与会话跟踪器 206 协作以收集活动会话及关联标识符的使用统计信息的组件示例。例如，标识符可以包括形式为网际协议地址或用户代理标识的请求位置。可以执行提取与收到的请求关联的统计信息 218 以提供与（在接收来自请求者的请求以形成收到的请求 216 中获取的）请求会话相关的信息集合，以便存储。如果基于异常的应用入侵检测系统 202 先前将此请求者检测为威胁，则可在提取与收到的请求

关联的统计信息 218 的操作期间提取额外的统计信息。

[0041] 规则 210 是能够在执行针对收到的请求的规则验证 220 时将传入请求的统计信息或特性及关联标识符与现有规则进行比较的组件示例。执行用于所使用的特定用户级别的规则的选择以识别相关规则。当获取请求时，通过对收到的请求执行规则验证 220 来根据预定的标准执行比较。在判定请求者是否为威胁 222 中，判定所述请求是否满足预定阈值。当所述比较不满足阈值时，在提升请求者的用户级别 224 中，将所述请求标记为可疑的。可疑请求一般被称为威胁。提升可疑请求将创建用于判定请求者验证是否成功 226 的新请求。当所述判定得出成功的结果时，执行针对收到的请求的规则验证 220，然后再次判定请求者是否为威胁 222。当没有任何威胁时，执行处理请求 230，并且过程在结束 232 处终止。

[0042] 对策 212 是系统内能够对已识别的威胁做出反应的组件示例。对策 212 表示可以发生增加用户识别和验证要求的位置示例。例如，提供对策作为阻止该请求 228。在另一示例中，最经常被置于 web 表单中以判定用户是否为人类并收集验证信息的挑战 - 应答测试也可以作为针对可疑攻击者或可疑用户提供的对策。

[0043] 现在参考图 3，其示出根据本发明的一个实施例与图 2 中的基于异常的应用入侵检测系统结合使用的提升增量和用户级别的方块图。提升增量 300 是包括不同提升级别的系统示例，其中每个级别需要不同于上一级别并且更具体的用户信息。

[0044] 图 2 中的检测系统 200 检测需要哪些级别，所述级别具有逐渐增加的用户信息披露和用户验证要求。当检测到威胁或异常时，强制将用户提升到下一级别。提升到下一级别包括增加用户身份和验证要求。通过提升用户身份和验证要求来防御应用层攻击具有多个优点，包括强制攻击者披露有关攻击者的更多信息。增加的信息通常会缩短识别攻击者所需的时间。由于许多应用层攻击是无意的，因此，使用提升增量 300 的过程可以有效地揭露攻击者的身份。对应用的其他用户的影响可以降到最低，因为验证过程是非侵入式的并且集成在应用中。使用提升增量 300 使得能够以编程的方式检测和阻止机器人或非人类代理的未授权访问。

[0045] 所述用户级别一般分为多个类别或用户级别 302，包括匿名 304、跟踪 306、认证 308、验证 310、信任 312 和阻止 314。匿名 304 是与其中用户不提供有关用户的任何特定信息的请求关联的类别。例如，如果这是发往网站的第一个请求的话。匿名请求被提升到跟踪 306 类别。如果请求属于可疑组，例如与特定网际协议地址或用户代理关联的已知恶意位置，则将所述请求提升到认证 308 用户级别。

[0046] 跟踪 306 表示属于在服务器层被安全跟踪的会话的请求。跟踪允许检测系统在特定代理使用应用的方式中检测异常，例如蛮力攻击或拒绝服务攻击。

[0047] 认证 308 表示当针对跟踪的请求发现异常时使用的跟踪 306 之后的下一更高级别，此时将强制代理进行认证。认证一般要求重定向到登录页面，在此要求用户提供身份并输入密码。所述登录页面通常被弄混乱以阻止机器人或其他自动用户的自动登录。作为另一示例，如果用户未在系统中注册，则系统可提供注册选项并在此时认证用户。系统可以执行验证并确保代理的注册信息完整。注册过程还可要求人类用户向系统提供更新的电话号码或电子邮件地址。

[0048] 验证 310 是当针对已认证的请求发现异常时使用的高于认证 308 的级别。在这种情况下，用户被提升到验证级别。验证 310 一般涉及使用人类验证工具或要求管理员或客

户服务代表对用户进行验证。所述工具确保呈现的用户不是诸如通过脚本编写的机器人之类的自动装置，并且当前访问该帐户的用户是最初注册该帐户的用户，或者是最初注册该帐户的用户所信任的用户。

[0049] 信任 312 表示这样一种用户级别，其中可信用户是指应用管理员已产生异常以始终被信任的用户。可信用户可以存在于所有级别中，例如，当匿名用户来自与可信机器人或管理员帐户关联的可信网际协议地址时，可信任该用户。

[0050] 阻止 314 表示其中阻止用户执行进一步操作的用户级别。与信任 312 相同，通过管理操作将用户设置为阻止，所述管理操作可以是自动执行的，也可以不是自动执行的。通常，阻止将响应于用户提交被判定为威胁的请求。例如，当重复使用一组网际协议地址来攻击某个站点时，属于这些地址的所有用户将被阻止。级别可以提升到或者随时被设为信任级别或阻止级别。向上提升遵循采用层次结构的路径，而设为特定级别使用入口点 316 以便直接访问。

[0051] 与不同的用户级别关联的安全性确定过程路径。可信用户级别是立即被处理的。当用户被阻止时，将阻止与所述用户关联的请求。匿名用户立即被提升到跟踪级别以提供附加信息。所有其他用户在被视为威胁时，将被提升到下一更高级别。在采取阻止操作之前，可给予用户多种机会来提升。阻止操作的条件或严重性将由管理员或安装定义的策略决定。

[0052] 参考图 4，其示出根据本发明的一个实施例使用图 3 中的提升增量的用户级别的阻止过程的流程图。过程 400 是使用图 3 中的提升增量 300 以及用户级别 302 的用户阻止过程的示例。

[0053] 过程 400 开始(步骤 402)并判定是否阻止请求(步骤 404)。当判定不阻止请求时，获取“否”响应。当判定阻止请求时，获取“是”响应。当在步骤 404 获取“否”时，在该示例中将用户级别 302 设为匿名 304。用户被自动提升到跟踪 306。当在步骤 404 获取“是”结果时，需要执行阻止操作并执行阻止请求(步骤 406)，之后过程 400 结束(步骤 418)。

[0054] 过程 400 判定请求是否为威胁(步骤 408)。可根据所跟踪的该用户或用户类型的信息与先前存储的信息的比较执行判定。所跟踪信息的比较基于比较与提升增量的用户级别关联的预定标准。当判定请求用户或请求为威胁时，获得“是”。当判定请求用户或请求不是威胁时，获得“否”结果。当在步骤 408 获得“否”结果时，未发现威胁并且在处理请求(步骤 416)中执行用户请求，之后过程 400 结束(步骤 418)。例如，当被跟踪的用户在网店上购物，并且用户尝试购买异常高数量的商品时，操作将触发“威胁”结果。

[0055] 当在步骤 408 获取“是”时，执行识别提升增量以形成已识别的提升(步骤 410)。选择提升增量可以根据用户级别层次结构中的下一级别或通过安装定义的策略做出。例如，默认设置可以允许用户级别向上渗入。在另一示例中，策略可根据给定的情况要求失败的认证导致将用户请求设为阻止。提升通常涉及增加用户身份和验证要求。

[0056] 执行使用已识别的提升增量进行提升(步骤 412)。执行的提升取决于分配给安装或用户管理员规范或选择所确定的相应用户级别的设置。判定提升是否成功(步骤 414)。当判定提升成功时，在步骤 414 获得“是”结果。当判定提升未成功时，在步骤 414 获得“否”结果。当在步骤 414 获得“是”结果时，过程 400 循环回到步骤 404，在该步骤重新评估用户请求。

[0057] 但是，当在步骤 414 获得“否”结果时，提升没有成功并且执行阻止请求的操作（步骤 406），之后过程 400 结束（步骤 418）。

[0058] 当请求提升或被设为验证 310 用户级别时，判定请求是否为威胁（步骤 420）。当判定请求为威胁时，获得“是”结果。当判定请求不是威胁时，获得“否”结果。当在步骤 420 获得“否”结果时，没有发现任何威胁并且在处理请求步骤 416 中执行用户请求，之后像上面一样，过程 400 在步骤 418 结束。当获得“是”结果时，在阻止请求 406 中执行阻止操作，之后像上面一样，过程 400 在步骤 418 结束。

[0059] 现在参考图 5a，其示出根据本发明的一个实施例的图 4 中的提升过程的流程图。过程 500 是与验证过程结合的提升过程的示例。例如，使用图 4 中已识别的提升增量提升用户级别以及通常执行的验证细节。

[0060] 过程 500 开始（步骤 502）并判定请求是否可信（步骤 504）。当判定请求可信时，获得“是”结果。当判定请求不可信时，获得“否”结果。当在步骤 504 获得“是”时，执行“执行请求”（步骤 520），之后过程 500 结束（步骤 534）。

[0061] 当在步骤 504 获得“否”时，判定是否阻止请求（步骤 506）。当判定阻止请求时，获得“是”结果。当判定不阻止请求时，获得“否”结果。当获得“是”结果时，执行阻止用户请求（步骤 508）。

[0062] 执行创建管理警报（步骤 510），之后过程 500 结束（步骤 534）。创建管理警报将记录阻止操作信息。例如，管理员或自动执行的过程可以使用管理警报日志将警报中所涉及的该用户设为图 3 中的阻止 314 级别。

[0063] 当在步骤 506 获得“否”结果时，将使用图 3 中的用户级别 302 进行提升。当从图 3 中用户级别 302 的匿名 304 级别进入时，将自动提升到图 3 中的跟踪 306 级别。在跟踪时，执行判定请求是否为威胁（步骤 512）。当判定请求为威胁时，获得“是”。当判定没有与请求关联的威胁时，获得“否”。当在步骤 512 获得“是”时，执行增强的认证方法（步骤 514）。提升过程可以包括进一步处理在跟踪与请求关联的会话期间收集的信息。例如，此时可能要求用户登录，并通过区分计算机和人类的全自动图灵测试（CAPTCHA）或一组安全提问以证明用户为人类用户，或者回答一组安全提问以支持用户身份。

[0064] 执行判定提升是否成功（步骤 516）。判定提升成功提供“是”结果。判定提升未成功提供“否”结果。当在步骤 516 获得“否”结果时，过程 500 像上面一样循环回到执行阻止请求（步骤 508）。当在步骤 516 获得“是”时，过程 500 循环回以重新评估请求并且像上面一样执行步骤 502。

[0065] 当从图 3 中用户级别 302 的认证 308 级别进入时，执行判定请求是否为威胁（步骤 518）。当判定存在威胁时，获得“是”结果。当判定没有威胁时，获得“否”结果。当在步骤 518 获得“否”时，像上面一样在步骤 520 执行处理请求。当在步骤 518 获得“是”时，过程 500 跳到步骤 524，该步骤将在下面的部分中描述并在图 5b 中示出。

[0066] 当从图 3 中用户级别 302 的验证 310 进入时，执行判定请求是否为威胁（步骤 522）。当判定存在威胁时，获得“是”结果。当判定没有威胁时，获得“否”结果。当在步骤 522 获得“否”时，像上面一样在步骤 520 执行处理请求，之后过程 500 结束（步骤 534）。当在步骤 522 获得“是”时，过程 500 循环回到阻止请求步骤 508。像上面一样，执行创建管理警报（步骤 510），之后过程 500 结束（步骤 534）。

[0067] 现在参考图 5b，其示出图 5a 的验证过程的流程图。当判定存在威胁，并且在步骤 518 获得“是”结果时，执行提示请求者进行验证（步骤 524）。需要请求者提供信息以帮助判定是否应当执行请求。信息可以是请求者唯一的个人相关信息或业务相关信息，或者是请求者了解的某种形式的特权信息。例如，所述信息可以包括帐户代码、出生日期、员工标识符和访问代码。提示还可以包括判定是否使用实时代理（live agent）的操作（步骤 526）。所述实时代理可以采取聊天会话或电话对话的形式。当判定使用实时代理时，获得“是”结果。当判定不使用实时代理时，获得“否”结果。

[0068] 当在步骤 526 获得“是”时，执行与实时代理对话（engage）（步骤 528）。所述代理开始与请求者进行对话以获得允许请求继续所需的信息。判定验证是否成功（步骤 530）。当判定验证成功时，获得“是”结果。当判定验证未成功时，获得“否”结果。

[0069] 当在步骤 530 获得“是”时，过程像上面一样循环回到步骤 502 中的重新评估请求。当在步骤 530 获得“否”时，过程 500 像上面一样循环回到步骤 508 中的阻止请求。过程 500 然后创建管理警报（步骤 510），之后结束（步骤 534）。

[0070] 当在步骤 526 获得“否”时，执行提示请求者提供所需的信息（步骤 532）。在这里，需要请求者输入缺失的信息以在可以处理请求之前用于进一步验证请求者。用户必须提供所需的信息来响应。例如，向请求者显示包括亮显输入字段的面板。请求者必须提供输入并进行验证以允许处理请求。像上面一样执行判定验证是否成功（步骤 530）。

[0071] 因此，说明性实施例提供了用于通过增加用户身份和验证要求来解决检测到的威胁的过程、计算机程序产品和装置。一个说明性实施例提供了计算机实现的用于解决检测到的威胁的过程，其接收来自请求者的请求以形成收到的请求并提取与所述收到的请求关联的统计信息以形成提取的统计信息。使用所述提取的统计信息对所述收到的请求执行规则验证并且响应于判定所述请求为威胁，使用提升增量提升所述请求者的级别，其中所述使用提升增量进一步包括通过渗入到下一用户级别和直接进入一个用户级别之一来增加用户身份和验证要求。

[0072] 例如，说明性实施例可以在机器人代理导致网站流量过大的情况下使用。业务合作伙伴可能正在尝试提取目录信息，实施机器人来扫描网站以及将每个产品添加到购物车以获得价格信息。计算价格是资源密集型操作。在短时间内执行数千次价格操作将导致服务停用，如果未被检测和管理的话。使用所述的过程，将强制业务合作伙伴进行认证，然后管理员便可了解是谁导致问题的产生。验证过程将可以阻止机器人代理工作，因此业务合作伙伴会注意到这点并自行决定与管理员联系。

[0073] 在另一示例中，业务用户尝试创建包括数百项商品的购物车。商店对于购物车中允许的最大商品数目没有固定的限制。购物车需要可产生存储器不足条件的大存储器占用。说明性实施例将在一旦检测到异常行为时强制用户登录。在验证提升期间，客户支持代表可以与用户进行对话。

[0074] 在另一示例中，使用上述说明性实施例，用户故意使用诸如注册功能之类的高冲击性应用功能攻击网站。恶意用户在注意到应用需要很长时间才能处理完大量注册请求后，创建数千个用户注册请求。用户不断地丢弃旧的会话以创建恶意攻击。上述说明性实施例将通过识别来自与攻击关联的特定用户代理的网际协议地址的用户组，来阻止匿名用户。

[0075] 附图中的流程图和方块图示出了根据本发明的各种实施例的系统、方法和计算机程序产品的可能实施方式的架构、功能和操作。在此方面，所述流程图或方块图中的每个方块都可以表示代码的模块、段或部分，所述代码包括用于实现指定的逻辑功能的一个或多个可执行指令。还应指出，在某些备选实施方式中，在方块中说明的功能可以不按图中说明的顺序发生。例如，示为连续的两个方块可以实际上被基本同时地执行，或者某些时候，取决于所涉及的功能，可以以相反的顺序执行所述方块。还应指出，所述方块图和 / 或流程图的每个方块以及所述方块图和 / 或流程图中的方块的组合可以由执行指定功能或操作的基于专用硬件的系统或专用硬件和计算机指令的组合来实现。

[0076] 下面权利要求中的所有装置或步骤加功能元件的对应结构、材料、操作和等同物旨在包括用于与其他所声明的元件结合执行所述功能的任何结构、材料或操作，如具体声明的那样。出于说明和描述目的给出了对本发明的描述，但是所述描述并非旨在是穷举的或是将本发明限于所公开的形式。在不偏离本发明的范围的情况下，许多修改和变化对于本领域的技术人员来说都将是显而易见的。实施例的选择和描述是为了最佳地解释本发明的原理、实际应用，并且当适合于所构想的特定使用时，使得本领域的其他技术人员能够理解本发明的具有各种修改的各种实施例。

[0077] 本发明可以采取完全硬件实施例、完全软件实施例或同时包含硬件和软件元素的实施例的形式。在优选实施例中，本发明在软件中实现，所述软件包括但不限于固件、驻留软件、微代码以及本领域的技术人员理解的其他软件介质。

[0078] 值得注意的是，尽管在全功能的数据处理系统中描述本发明，但是本领域的技术人员将理解，本发明的过程能够以指令的计算机可读介质的形式以及各种形式进行分发，并且本发明不管实际用于执行分发的特定信号承载介质类型是同等适用的。计算机可读介质的示例包括诸如软盘、硬盘驱动器、RAM、CD-ROM、DVD-ROM 之类的可记录类型介质以及诸如数字和模拟通信链路、有线或使用例如射频和光波传输等传输形式的无线通信链路之类的传输类型介质。所述计算机可读介质可以采取编码格式的形式，所述编码格式被解码以实际用于特定的数据处理系统。

[0079] 适合于存储和 / 或执行程序代码的数据处理系统将包括至少一个通过系统总线直接或间接连接到存储器元件的处理器。所述存储器元件可以包括在程序代码的实际执行期间采用的本地存储器、大容量存储装置以及提供至少某些程序代码的临时存储以减少必须在执行期间从大容量存储装置检索代码的次数的高速缓冲存储器。

[0080] 输入 / 输出或 I/O 设备(包括但不限于键盘、显示器、指点设备等)可以直接或通过中间 I/O 控制器与系统相连。

[0081] 网络适配器也可以被连接到系统以使所述数据处理系统能够通过中间专用或公共网络变得与其他数据处理系统或远程打印机或存储设备相连。调制解调器、电缆调制解调器和以太网卡只是几种当前可用的网络适配器类型。

[0082] 出于说明和描述目的给出了对本发明的描述，并且所述描述并非旨在是穷举的或是将本发明限于所公开的形式。许多修改和变化对于本领域的技术人员来说都将是显而易见的。实施例的选择和描述是为了最佳地解释本发明的原理、实际应用，并且当适合于所构想的特定使用时，使得本领域的其他技术人员能够理解本发明的具有各种修改的各种实施例。

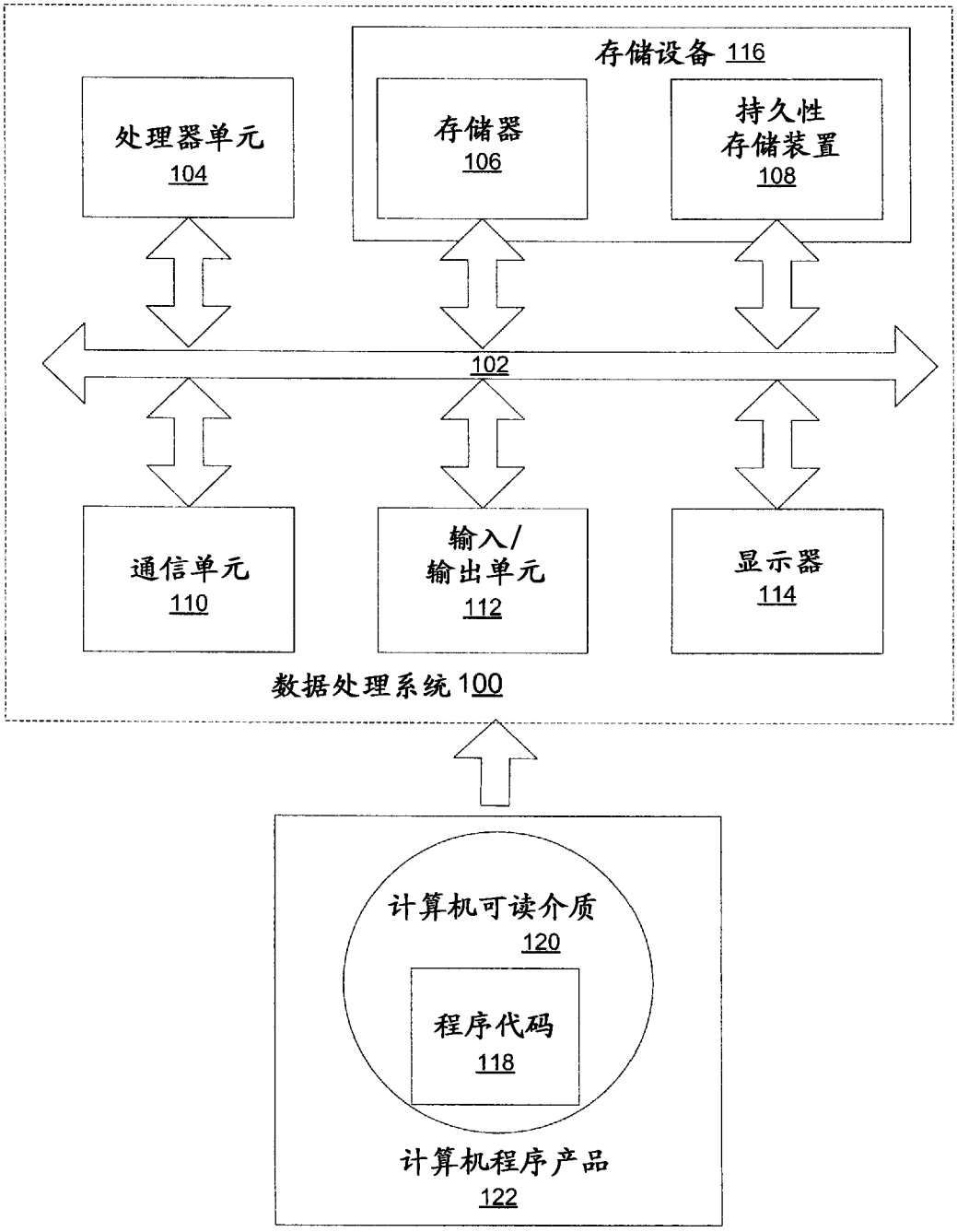

存储设备 116
处理器单元
104
存储器
106
持久性
存储装置
108
102
通信单元
110
输入/
输出单元
112
显示器
114
数据处理系统 100
计算机可读介质
120
程序代码
118
计算机程序产品
122

图 1

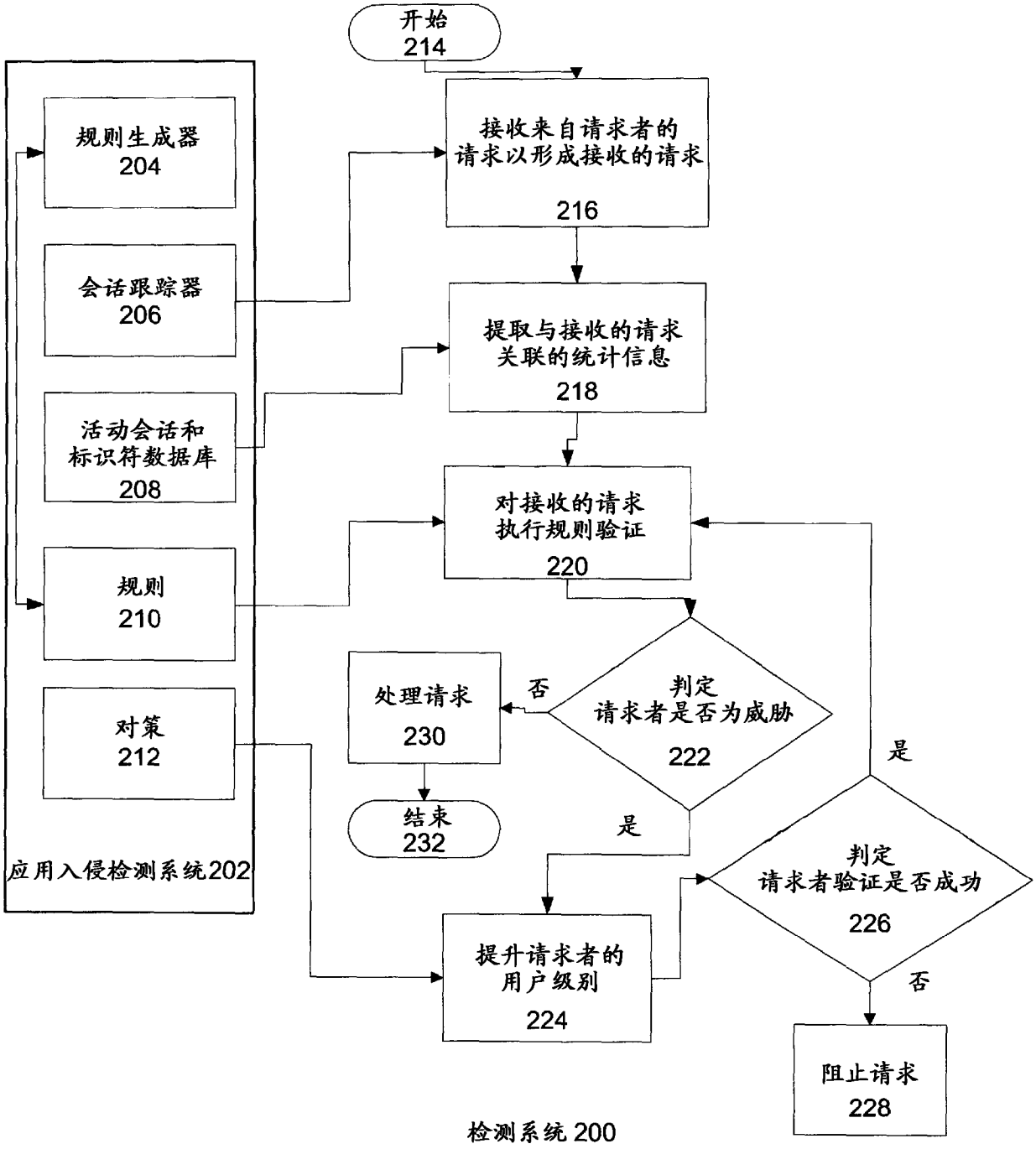

开始
214
接收来自请求者的请求以形成接收的请求
216
提取与接收的请求关联的统计信息
218
对接收的请求执行规则验证
220
判定请求者是否为威胁
222
否
处理请求
230
结束
232
是
判定请求者验证是否成功
226
是
否
提升请求者的用户级别
224
阻止请求
228
规则生成器
204
会话跟踪器
206
活动会话和标识符数据库
208
规则
210
对策
212
应用入侵检测系统202
检测系统 200

图 2

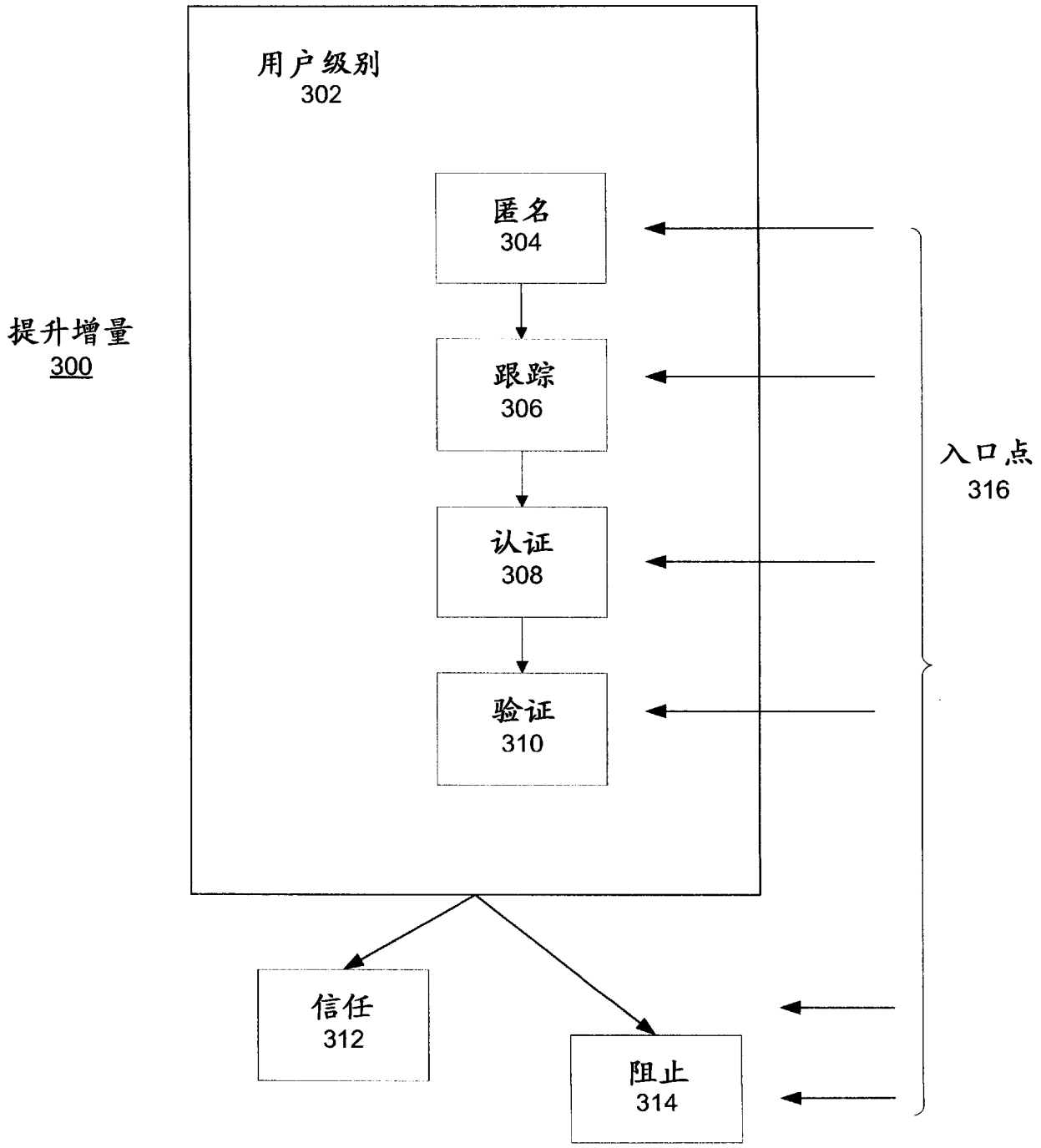

用户级别
302
匿名
304
跟踪
306
认证
308
验证
310
提升增量
300
入口点
316
信任
312
阻止
314

图 3

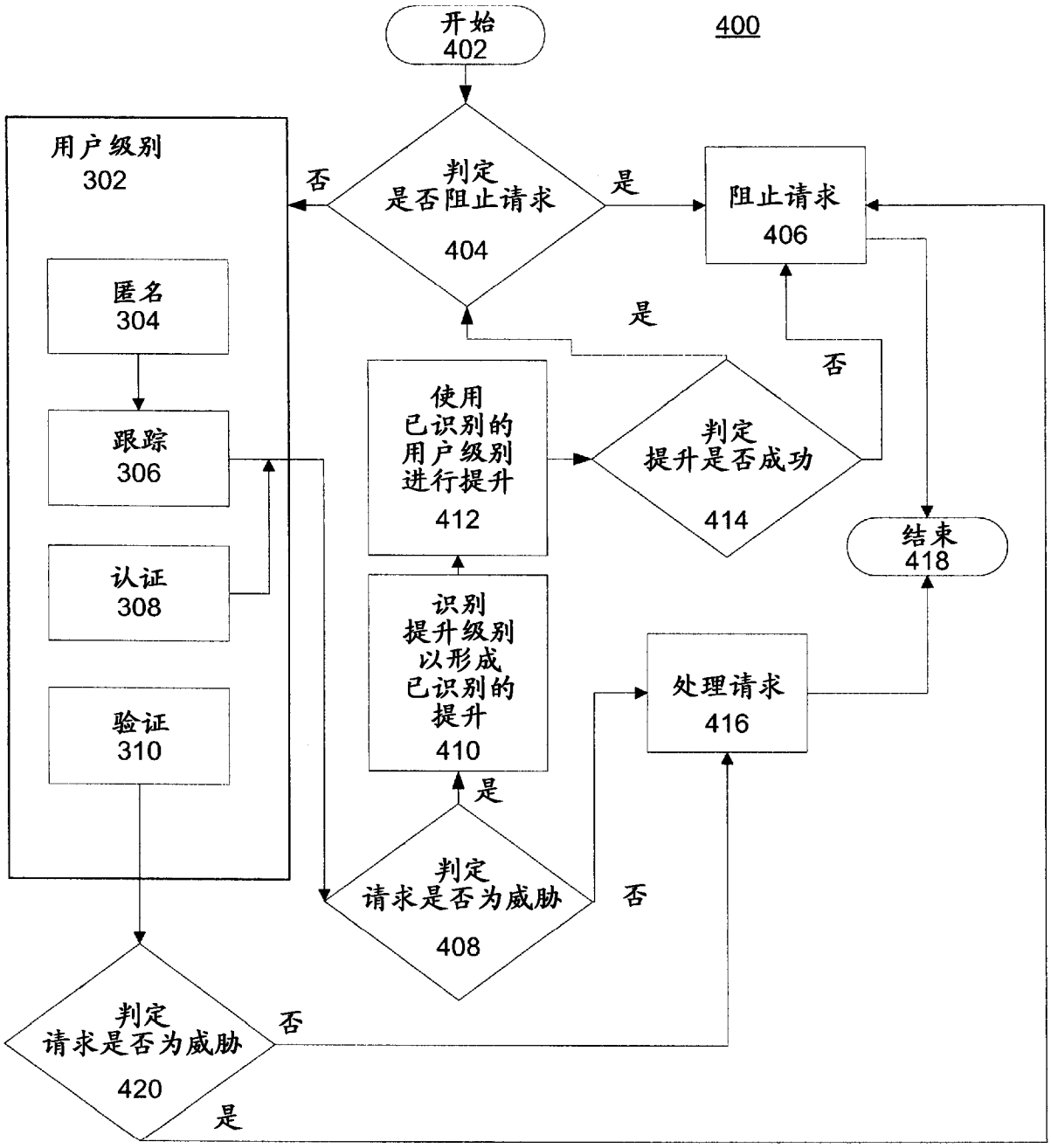

开始
402
400
用户级别
302
判定
是否阻止请求
404
否
是
阻止请求
406
匿名
304
跟踪
306
认证
308
验证
310
使用
已识别的
用户级别
进行提升
412
判定
提升是否成功
414
是
否
结束
418
识别
提升级别
以形成
已识别的
提升
410
处理请求
416
是
判定
请求是否为威胁
408
否
判定
请求是否为威胁
420
否
是

图 4

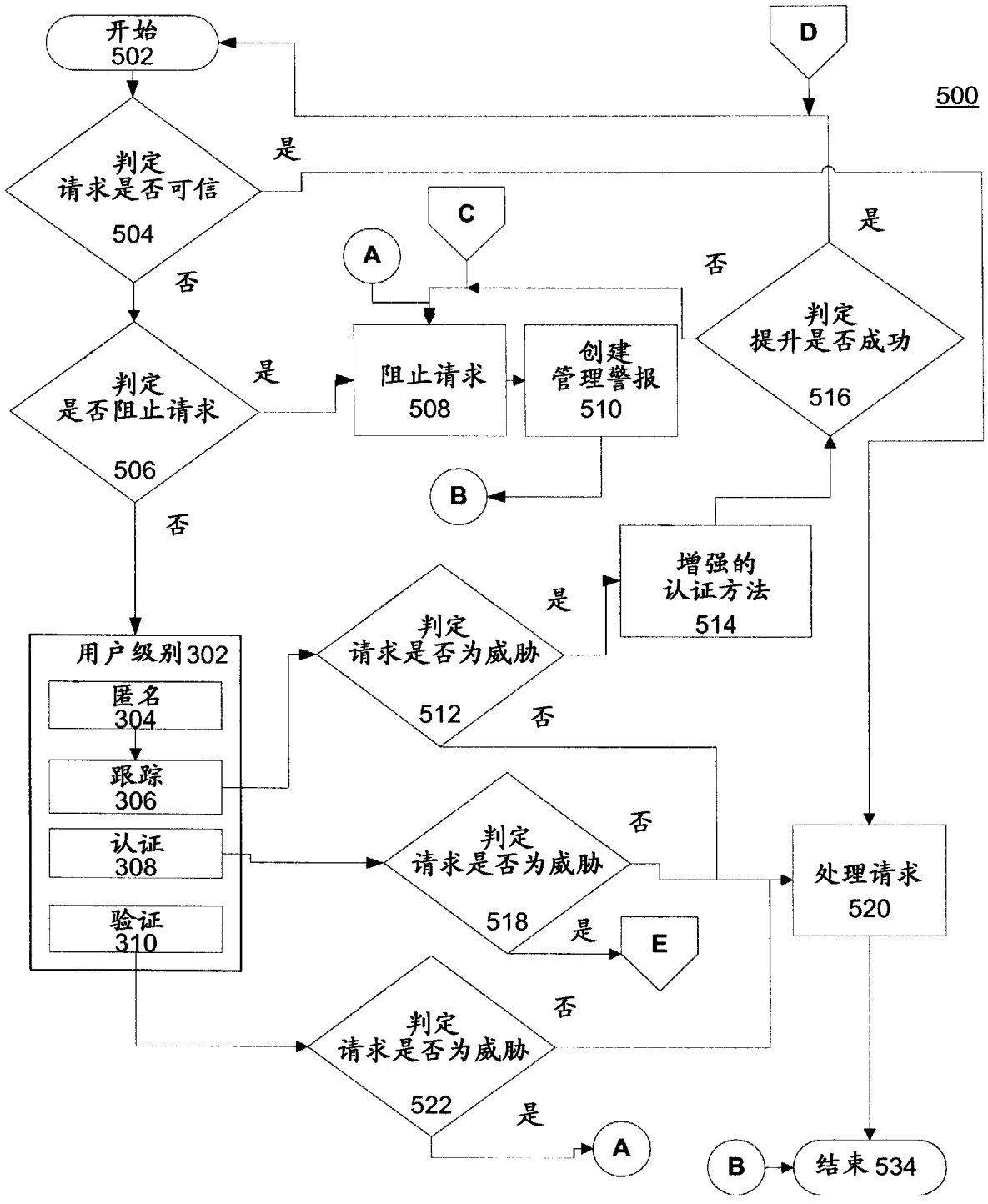

开始
502
D
500
判定
请求是否可信
504
是
否
C
A
是
否
判定
提升是否成功
516
判定
是否阻止请求
506
是
阻止请求
508
创建
管理警报
510
B
否
增强的
认证方法
514
是
判定
请求是否为威胁
512
否
用户级别302
匿名
304
跟踪
306
认证
308
验证
310
判定
请求是否为威胁
518
否
是
E
处理请求
520
判定
请求是否为威胁
522
否
是
A
B
结束534

图 5a

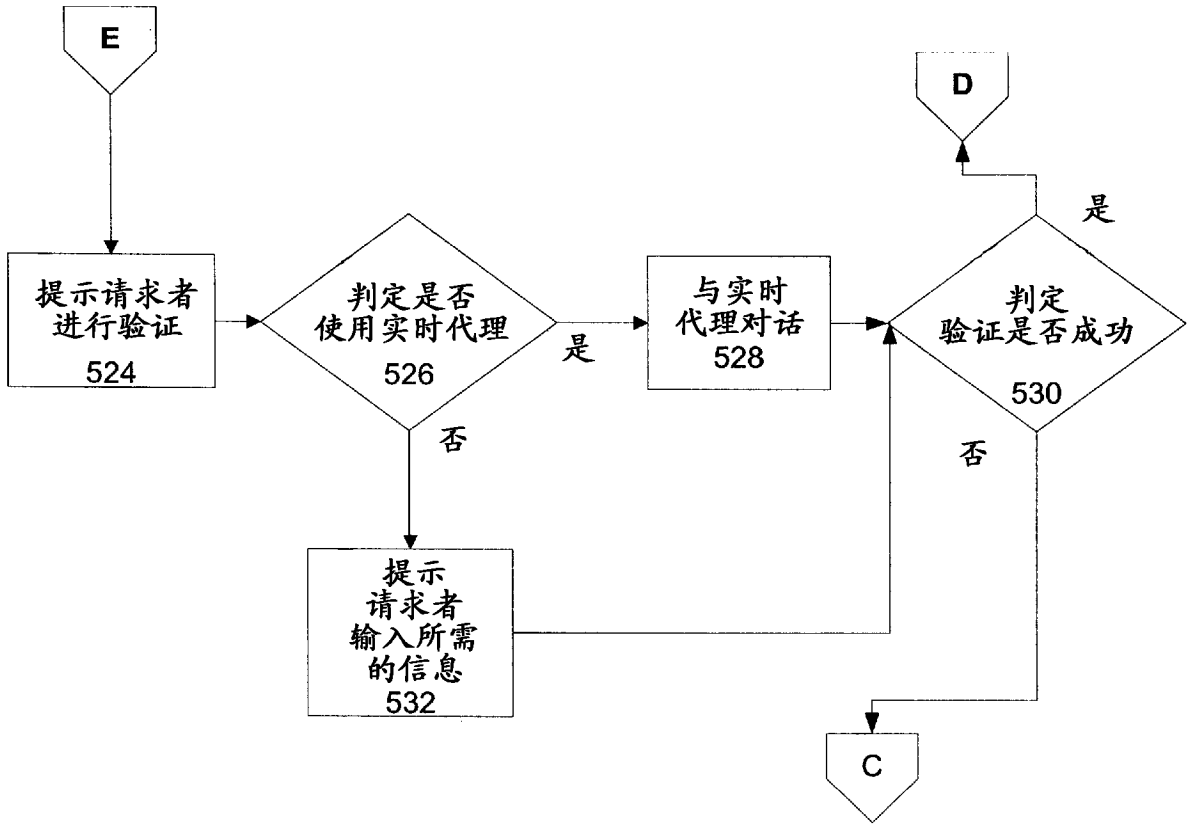

E
提示请求者
进行验证
524
判定是否
使用实时代理
526
是
否
与实时
代理对话
528
判定
验证是否成功
530
是
否
D
提示
请求者
输入所需
的信息
532
C

图 5b