(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 107211016 B
(45)授权公告日 2020.10.30

(21)申请号 201680006399.1
(22)申请日 2016.01.19
(65)同一申请的已公布的文献号
申请公布号 CN 107211016 A
(43)申请公布日 2017.09.26
(30)优先权数据
62/105,685 2015.01.20 US
14/827,230 2015.08.14 US
(85)PCT国际申请进入国家阶段日
2017.07.19
(86)PCT国际申请的申请数据
PCT/US2016/013942 2016.01.19
(87)PCT国际申请的公布数据
WO2016/118517 EN 2016.07.28
(73)专利权人 赛姆普蒂夫技术公司
地址 美国华盛顿州
(72)发明人 罗伯特·派克
(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 唐京桥 陈炜
(51)Int.Cl.
H04L 29/06(2006.01)
(56)对比文件
US 2005188222 A1,2005.08.25
US 2005188222 A1,2005.08.25
US 2012240185 A1,2012.09.20
CN 101741832 A,2010.06.16
CN 103051623 A,2013.04.17
US 2012131204 A1,2012.05.24
US 2002184217 A1,2002.12.05
审查员 陈翠莹

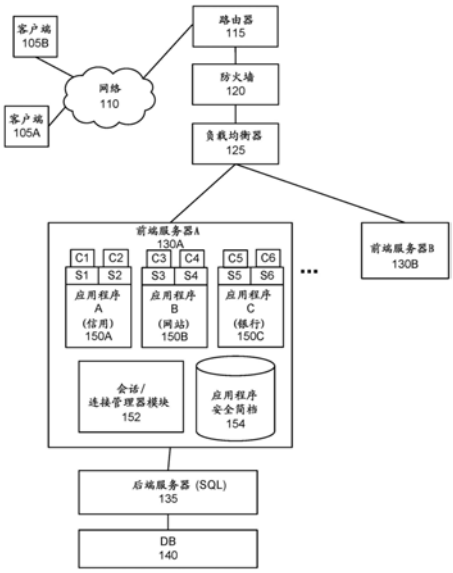
权利要求书3页 说明书10页 附图9页

(54)发明名称

会话安全划分和应用程序剖析器

(57)摘要

提供防御黑客的在线安全的智能方法,其防止黑客获得对安全资源的未授权访问。检测在第一客户端与第一主机设备的第一应用程序之间建立的第一应用程序会话。第一应用程序与将第一应用程序的安全性划分成安全层的第一多个安全时间限制相关联。监测在第一客户端与第一应用程序之间建立的第一应用程序会话的持续时间。响应于第一应用程序会话的持续时间达到第一多个安全时间限制中的安全时间限制,对第一应用程序会话执行一个或更多个第一安全动作。响应于第一应用程序会话的持续时间达到第一多个安全时间限制中的另一安全时间限制,对第一应用程序会话执行一个或更多个第二安全动作。



CN 107211016 B

1.一种用于防止对资源的未授权访问的计算机实现的方法,包括:

监测对应于第一应用程序的多个应用程序会话的持续时间,以生成会话持续时间数据;

基于所述会话持续时间数据来确定第一多个安全时间限制,所述第一多个安全时间限制将所述第一应用程序的安全性划分成安全层;

检测在第一客户端与所述第一应用程序之间建立的第一应用程序会话;

监测在所述第一客户端与所述第一应用程序之间建立的第一应用程序会话的持续时间;

响应于所述第一应用程序会话的持续时间达到所述第一多个安全时间限制中的安全时间限制,对所述第一应用程序会话执行一个或更多个第一安全动作;以及

响应于所述第一应用程序会话的持续时间达到所述第一多个安全时间限制中的另一安全时间限制,对所述第一应用程序会话执行一个或更多个第二安全动作,

其中,所述第一安全动作或所述第二安全动作之一包括:通过将所述第一应用程序会话从第一主机设备移动到第二主机设备来将所述第一应用程序会话与和所述第一主机设备相关联的其它应用程序会话隔离。

2.根据权利要求1所述的方法,还包括:

检测在第二客户端与所述第一主机设备的第二应用程序之间建立的第二应用程序会话,所述第二应用程序与第二多个安全时间限制相关联,所述第二多个安全时间限制将应用程序的安全性划分成安全层;

监测在所述第二客户端与所述第二应用程序之间建立的第二应用程序会话的持续时间;

响应于所述第二应用程序会话的持续时间达到所述第二多个安全时间限制中的安全时间限制,对所述第二应用程序会话执行所述一个或更多个第一安全动作;以及

响应于所述第二应用程序会话的持续时间达到所述第二多个安全时间限制中的另一安全时间限制,对所述第二应用程序会话执行所述一个或更多个第二安全动作。

3.根据权利要求1所述的方法,其中,所述第一安全动作或所述第二安全动作之一包括IP查找、深度数据包检查、畸形数据包检测或启用蜜罐安全传感器之一。

4.根据权利要求1所述的方法,其中,第一会话是开放系统互连(OSI)会话层的会话。

5.一种非暂态计算机可读介质,其存储用于防止对资源的未授权访问的指令,所述指令在由至少一个处理器执行时使所述至少一个处理器执行以下操作:

监测对应于第一应用程序的多个应用程序会话的持续时间,以生成会话持续时间数据;

基于所述会话持续时间数据来确定第一多个安全时间限制,所述第一多个安全时间限制将所述第一应用程序的安全性划分成安全层;

检测在第一客户端与所述第一应用程序之间建立的第一应用程序会话;

监测在所述第一客户端与所述第一应用程序之间建立的第一应用程序会话的持续时间;

响应于所述第一应用程序会话的持续时间达到所述第一多个安全时间限制中的安全时间限制,对所述第一应用程序会话执行一个或更多个第一安全动作;以及

响应于所述第一应用程序会话的持续时间达到所述第一多个安全时间限制中的另一安全时间限制，对所述第一应用程序会话执行一个或更多个第二安全动作，

其中，所述第一安全动作或所述第二安全动作之一包括：通过将所述第一应用程序会话从第一主机设备移动到第二主机设备来将所述第一应用程序会话与和所述第一主机设备相关联的其它应用程序会话隔离。

6.一种用于防止对资源的未授权访问的计算机实现的方法，包括：

监测针对与第一应用程序对应的会话建立的多个连接的持续时间，以生成连接持续时间数据；

基于所述连接持续时间数据来确定第一多个安全时间限制，所述第一多个安全时间限制将所述第一应用程序的安全性划分成安全层；

检测针对第一客户端与所述第一应用程序之间的第一会话建立的第一连接；

监测在所述第一客户端与所述第一应用程序之间建立的第一连接的持续时间；

响应于所述第一连接的持续时间达到与所述第一应用程序相关联的第一多个安全时间限制中的安全时间限制，对所述第一连接执行一个或更多个第一安全动作；以及

响应于所述第一连接的持续时间达到所述第一多个安全时间限制中的另一安全时间限制，对所述第一连接执行一个或更多个第二安全动作，

其中，所述第一安全动作或所述第二安全动作之一包括：通过将所述第一连接从第一主机设备移动到第二主机设备来将所述第一连接与和所述第一主机设备相关联的其它连接隔离。

7.根据权利要求6所述的方法，还包括：

检测针对第二客户端与所述第一主机设备的第二应用程序之间的第二会话建立的第二连接，所述第二应用程序与第二多个安全时间限制相关联，所述第二多个安全时间限制将所述第二应用程序的安全性划分成安全层；

监测第二连接的持续时间；

响应于所述第二连接的持续时间达到所述第二多个安全时间限制中的安全时间限制，对所述第二连接执行所述一个或更多个第一安全动作；以及

响应于所述第二连接的持续时间达到所述第二多个安全时间限制中的另一安全时间限制，对所述第二连接执行所述一个或更多个第二安全动作。

8.根据权利要求6所述的方法，其中，所述第一安全动作或所述第二安全动作之一包括IP查找、深度数据包检查、畸形数据包检测或启用蜜罐安全传感器。

9.根据权利要求6所述的方法，其中，所述第一连接是TCP连接。

10.一种非暂态计算机可读介质，其存储用于防止对资源的未授权访问的指令，所述指令在由至少一个处理器执行时使所述至少一个处理器执行以下操作：

监测针对与第一应用程序对应的会话建立的多个连接的持续时间，以生成连接持续时间数据；

基于所述连接持续时间数据来确定第一多个安全时间限制，所述第一多个安全时间限制将所述第一应用程序的安全性划分成安全层；

检测针对第一客户端与所述第一应用程序之间的第一会话建立的第一连接；

监测在所述第一客户端与所述第一应用程序之间建立的第一连接的持续时间；

响应于所述第一连接的持续时间达到与所述第一应用程序相关联的第一多个安全时间限制中的安全时间限制,对所述第一连接执行一个或更多个第一安全动作;以及

响应于所述第一连接的持续时间达到所述第一多个安全时间限制中的另一安全时间限制,对所述第一连接执行一个或更多个第二安全动作,

其中,所述第一安全动作或所述第二安全动作之一包括:通过将所述第一连接从第一主机设备移动到第二主机设备来将所述第一连接与和所述第一主机设备相关联的其它连接隔离。

11.根据权利要求10所述的非暂态计算机可读介质,其中,所述操作还包括:

检测在第二客户端与所述第一主机设备的第二应用程序之间建立的第二应用程序会话,所述第二应用程序与第二多个安全时间限制相关联,所述第二多个安全时间限制将应用程序的安全性划分成安全层;

监测在所述第二客户端与所述第二应用程序之间建立的第二应用程序会话的持续时间;

响应于所述第二应用程序会话的持续时间达到所述第二多个安全时间限制中的安全时间限制,对所述第二应用程序会话执行所述一个或更多个第一安全动作;以及

响应于所述第二应用程序会话的持续时间达到所述第二多个安全时间限制中的另一安全时间限制,对所述第二应用程序会话执行所述一个或更多个第二安全动作。

12.根据权利要求10所述的非暂态计算机可读介质,其中,所述第一安全动作或所述第二安全动作之一包括IP查找、深度数据包检查、畸形数据包检测或启用蜜罐安全传感器之一。

13.根据权利要求10所述的非暂态计算机可读介质,其中,第一会话是开放系统互连(OSI)会话层的会话。

14.根据权利要求10所述的非暂态计算机可读介质,其中,所述操作还包括:

检测针对第二客户端与所述第一主机设备的第二应用程序之间的第二会话建立的第二连接,所述第二应用程序与第二多个安全时间限制相关联,所述第二多个安全时间限制将所述第二应用程序的安全性划分成安全层;

监测第二连接的持续时间;

响应于所述第二连接的持续时间达到所述第二多个安全时间限制中的安全时间限制,对所述第二连接执行所述一个或更多个第一安全动作;以及

响应于所述第二连接的持续时间达到所述第二多个安全时间限制中的另一安全时间限制,对所述第二连接执行所述一个或更多个第二安全动作。

15.根据权利要求10所述的非暂态计算机可读介质,其中,所述第一连接是TCP连接。

会话安全划分和应用程序剖析器

[0001] 相关申请的交叉引用

[0002] 本申请要求于2015年1月20日提交的美国临时专利申请第62/105,685号的优先权,通过引用将其全部内容并入。

技术领域

[0003] 本公开涉及防御对资源的未授权访问的计算机安全,更具体地,涉及剖析应用程序并将这些应用程序的会话和连接划分成安全层。

背景技术

[0004] 在网络通信中,存在多种形式的软件安全和硬件安全,包括防火墙以及入侵检测和预防系统。但是,它们都在一个核心问题上存在问题,即,如果规则没有被正确地应用,则它们会给未授权访问提供机会。当今的操作系统和应用程序也有许多错误,如果暴露在因特网上,则这些错误会允许对托管应用程序的服务器的远程访问。

[0005] 现有的防火墙支持数据包检测。该检测基于应用于防火墙中的配置的规则,并且在主动学习方面具有局限性,原因是它们不能与应用程序堆栈对话,并且应用程序堆栈具有有限的与安全堆栈对话的能力。防火墙通常会试图并减少规则的数量,原因是如果应用太多的规则,则在与主机的每个连接上会产生巨大的开销,并且在大规模的情况下可能会有问题。

发明内容

[0006] 本公开的实施方式包括提供防御黑客的在线安全的智能方法,其防止黑客获得对安全资源的未授权访问。在一个实施方式中,公开了一种防御对资源的未授权访问的安全方法。检测在第一客户端与第一主机设备的第一应用程序之间建立的第一应用程序会话。第一应用程序与将第一应用程序的安全性划分成安全层的第一多个安全时间限制相关联。监测在第一客户端与第一应用程序之间建立的第一应用程序会话的持续时间。响应于第一应用程序会话的持续时间达到第一多个安全时间限制中的安全时间限制,对第一应用程序会话执行一个或更多个第一安全动作。响应于第一应用程序会话的持续时间达到第一多个安全时间限制中的另一安全时间限制,对第一应用程序会话执行一个或更多个第二安全动作。

[0007] 在一个实施方式中,通过机器学习过程建立安全时间限制。该过程可以包括监测与第一应用程序相对应的多个先前应用程序会话的持续时间,以生成第一会话持续时间数据。然后,基于多个先前应用程序会话的第一会话持续时间数据来确定第一多个安全时间限制。

[0008] 在一个实施方式中,所述方法还包括:检测在第二客户端与至少一个服务器的第二应用程序之间建立的第二应用程序会话,第二应用程序与将第二应用程序的安全性划分成安全层的第二多个安全时间限制相关联;监测在第二客户端与第二应用程序之间建立的

第二应用程序会话的持续时间;响应于第二应用程序会话的持续时间达到所述多个安全时间限制中的安全时间限制,对第二应用程序会话执行一个或更多个第一安全动作;以及响应于第二应用程序会话的持续时间达到所述多个安全时间限制中的另一安全时间限制,对第二应用程序会话执行一个或更多个第二安全动作。

[0009] 在一个实施方式中,第一安全动作或第二安全动作之一包括IP查找、深度数据包检查、畸形数据包检测或启用蜜罐安全传感器中至少之一。在一个实施方式中,第一安全动作或第二安全动作之一包括:将第一应用程序会话与和至少一个主机设备相关联的其他应用程序会话隔离。隔离第一应用程序会话可以包括将第一应用程序会话移动至第二主机设备。隔离第一应用程序会话还可以包括将第一应用程序会话保持在第一主机设备上,并且防止与第一主机设备建立其他应用程序会话。

[0010] 在一个实施方式中,在线安全的方法也可以应用于为应用程序会话建立的连接。其他实施方式包括存储指令的非暂态计算机可读介质。所述指令可由至少一个处理器执行以实现用于防止对资源的未授权访问的操作。

附图说明

[0011] 图1是根据实施方式的具有会话/连接划分的网络通信系统的框图。

[0012] 图2是根据实施方式的被划分成不同安全层的应用程序会话/连接的示图。

[0013] 图3是根据实施方式的被划分成不同安全层的不同应用程序的应用程序会话/连接的示图。

[0014] 图4是示出根据实施方式的应用程序会话/连接的隔离的示图。

[0015] 图5是示出根据另一实施方式的应用程序会话/连接的隔离的示图。

[0016] 图6是根据实施方式的来自图1的会话/连接管理器模块的框图。

[0017] 图7是根据实施方式的用于剖析应用程序的会话/连接以及时间限制的学习的方法的流程图。

[0018] 图8是根据实施方式的用于会话/连接划分安全的方法的流程图。

[0019] 图9示出了根据实施方式的计算设备的硬件架构。

具体实施方式

[0020] 现在将详细参考本公开的若干实施方式,其示例在附图中示出。应注意,在可行的情况下,可以在附图中使用类似或相似的附图标记,并且类似或相似的附图标记可以指代类似或相似的功能。附图仅出于说明的目的来描述本公开的实施方式。本领域技术人员将从以下描述中容易地认识到,在不脱离本文所述的公开内容的原理或得到的益处的情况下,可以采用本文所示的结构和方法的替代实施方式。

[0021] 未来的对在线应用程序的保护基于安全性的机器层面的学习以及允许安全系统剖析平均应用程序会话流。平均应用程序会话流可以改变多级触发会话的触发点。会话持续时间越长,会话所具有的风险越高。本公开的实施方式将剖析会话,并且将根据时间或状态来启动安全动作,例如通过分析异常数据包流的会话或复制数据包流以用于在受控分析安全沙箱中回放。

[0022] 本公开的实施方式涉及安全系统平台的组件,其剖析应用程序以防止黑客访问后

端数据集并防止对任何数据集的持续访问。本公开的实施方式还将在应用程序和网络中发现的各种应用程序会话划分成单个会话内的安全层/片段，并且随时间增加每个安全层/片段的安全级别。更具体地，本公开的实施方式可以通过使用更高安全性解决方案的升级的安全级别来防止对未授权资源的访问。本公开的实施方式还可以将连接划分成安全层，并且随时间增加每个安全层的安全级别。

[0023] 图1是根据实施方式的具有会话划分安全和连接划分安全的网络通信系统的框图。系统包括若干客户端设备105、网络110、路由器115、防火墙120、负载均衡器125、前端服务器130、后端服务器135和数据库140。计算设备例如路由器115、防火墙120、负载均衡器125、前端服务器130、后端服务器135和数据库140可以形成由客户端105经由网络110访问的数据中心。为了便于说明，在图1中仅示出了两个客户端105和两个前端服务器130。在其他实施方式中，可以存在更多数量的客户端设备105和前端服务器130。

[0024] 客户端设备105可以是计算设备，例如智能电话、平板计算机、膝上型计算机和台式计算机等。用户通过诸如触摸屏或鼠标和键盘的接口与客户端设备105的软件进行交互。客户端设备105由用户控制以建立与由前端服务器130托管的各种应用程序的应用程序会话和连接。

[0025] 前端服务器130是可以包括一个或更多个处理器并执行操作系统的服务器类计算设备。服务器130托管若干软件应用程序150，并且在本文中也可以被称为主机设备。例如，应用程序150可以托管信用卡支付应用程序150A、网站150B和网上银行应用程序150C。托管应用程序150的主机设备的其他示例可以是通用电子设备、电话、平板电脑、飞机中的飞行控制系统等。

[0026] 客户端设备105可以经由网络110、路由器115、防火墙和负载均衡器125与应用程序150建立网络连接C1-C6。连接被用作在服务器150和客户端设备105处的套接字(socket)之间的双向通信信道。连接在一定时间点建立，例如使用握手或有时没有握手过程，然后在稍后的时间点终止。连接可以包括由协议定义的若干状态。一种类型的连接示例是在开放系统互连(OSI)模型的传输层下的传输控制协议(TCP)连接。

[0027] 客户端设备105还通过连接C1-C6与应用程序150建立应用程序会话S1-S6。应用程序会话是给定应用程序的两个或更多个通信实体之间的交互式信息交换。应用程序会话在一定时间点建立，然后在稍后的时间点终止。在应用程序会话期间，可以通过已经为会话建立的连接在每个方向上发送请求信息或响应于请求的一个或更多个消息。会话的状态(例如登录、注销、空闲、上传、下载、搜索、处理或更新现有数据、破坏或删除数据、触发警报、时间计数器状态、密钥匹配、密钥更改、风险因素状态)可以由前端服务器130A或客户端105维护。在一个实施方式中，应用程序会话是位于传输层之上的OSI会话层的会话。会话的示例可以是HTTP会话、FTP会话和SMTP会话等。

[0028] 在一个示例中，当用户在客户端设备105A处刷信用卡时，可以发起信用卡认证会话(例如，S1、S2)，并且客户端设备105A与信用卡支付应用程序150A建立连接和会话。信用卡支付应用程序150A与客户端设备105A进行通信，以从客户端设备105A取得信用卡号码和收费金额。然后，信用卡支付应用程序150A经由后端服务器135访问数据库140，以确定信用卡号码是否具有足够的信用以处理支付。然后，信用卡支付应用程序150A向客户端设备105A提供肯定响应/否定响应。然后，在向客户端设备105A提供响应之后终止连接和会话。

[0029] 在另一示例中，当用户在客户端105B处将URL输入到浏览器中时，可以发起网络表单会话(例如，S3、S4)。客户端设备105B与网站150B建立会话。前端服务器130A(即，网络服务器)可以处理多个会话。前端服务器130A每个会话启动时间计数器。用户在会话关闭前有x时间量填写表单。由于填写网络表单数据所花费的时间，不同的前端服务器130B可以处理来自初始会话的表单提交。

[0030] 在另一示例中，当用户在客户端设备105B处打开移动银行应用程序时，可以发起网上银行会话(例如S5、S6)，并且客户端设备105B与网上银行应用程序150C建立连接和会话。网上银行应用程序150C与客户端设备105C进行通信，以从客户端设备105C获得认证信息。一旦得到认证，客户端设备105C可以请求帐户余额，上传存款票据的副本，以及进行其他银行请求。银行应用程序150C可以经由后端服务器135访问存储在数据库140中的帐户信息以处理这些请求。

[0031] 后端服务器135提供对存储在数据库140中的数据的访问。应用程序150中的任何应用程序可以从后端服务器135请求数据，然后后端服务器135从数据库140检索数据并将数据提供给应用程序150。后端服务器135的示例是SQL服务器。黑客经常试图通过被入侵的会话或连接访问数据库140中的数据，而会话/连接管理器模块152试图在成功访问数据之前检测这些被入侵的会话和连接。在被操纵的会话的情况下，黑客将会延长会话的时间表，这是风险因素增加的地方，而会话/连接管理器模块152可以增加安全性并触发警报。

[0032] 会话/连接管理器模块152提供针对被入侵的会话/连接的安全性。对于每个会话/连接，会话/连接管理器模块152将会话/连接划分成不同的时间触发的安全层。通过强制将会话/连接按时间划分为安全层，可以基于单个会话/连接的划分层触发不同的动作。在每个层中，会话/连接管理器模块152向会话/连接施加一个或更多个安全动作。在一个实施方式中，通过执行用于处理单元(例如，处理器或控制器或定制应用程序专用集成电路)上的安全动作的软件程序代码，针对会话/连接应用安全动作。

[0033] 安全动作可以是被设计成通过分析来自会话的数据来检测黑客或防止黑客成功地完成入侵的动作。安全动作的示例可以包括IP查找、激活蜜罐传感器、会话/连接隔离、深度数据包检查、遏制会话/连接、发出安全警报、会话/连接跟踪、会话/连接记录、将机器学习应用于会话/连接和完全控制/提醒及终止会话/连接。较早的安全层可以包括不同的规则，并且可以被配置成具有很少甚至没有安全动作以减少误报，而后来的安全层可以包括更多的资源密集型安全动作。在后来的安全层中，会话/连接管理器模块152可以通知其他设备(例如路由器115、防火墙120或负载均衡器125)高风险安全会话/连接，并且使得其他设备将安全动作施加至会话/连接。

[0034] 会话/连接管理器模块152监测会话/连接的持续时间，然后一旦会话/连接持续时间达到一定安全时间限制，则将安全性从一个安全层提升到下一个安全层。大多数正常会话/连接预计在达到安全时间限制之前完成。只有被入侵的会话/连接预计会超出安全时间限制。因此，更多的资源密集型安全动作仅施加至处于被入侵会话的较高风险的会话/连接。因此，根据时间提升安全层具有如下技术优点：通过减小计算硬件(例如，处理器和存储器)上的计算负担来改善前端服务器130的功能，通过在会话的特定时间段内有条理地提升安全层来改善前端服务器130的功能，同时仍然保持防御黑客的高水平的安全性。

[0035] 在不同的时间间隔中具有不同的安全动作还使得工具能够理解什么是正常会话，

什么是被入侵的会话，并且相应地终止、跟踪、追踪、记录、升级、分析会话的状态。此外，连接和会话最终基于黑客离开或被迫离开而在会话结束时终止。当黑客返回时，可以使用从黑客以前的入侵尝试中剖析的某些指纹数据来识别黑客，并立即升级风险级别，这会触发记录或应用更多的安全传感器，同时系统了解了黑客如何试图升级他对主机或后端系统的访问权限。一旦连接的会话状态被去除/终止，机器学习可以自行纠正发现的漏洞并终止会话以阻止黑客。

[0036] 对于每种类型的应用程序150，安全时间限制可以是不同的。在一个实施方式中，会话/连接管理器模块152经由机器学习过程单独针对每个应用程序确定安全时间限制。学习过程监测应用程序的先前会话/连接持续时间，根据会话/连接持续时间生成会话/连接持续时间数据，并将会话/连接持续时间数据存储在应用程序安全简档数据库154中的应用程序安全简档中。然后，可以根据应用程序的应用程序安全简档中的会话/连接持续时间数据确定应用程序的会话/连接的安全时间限制，这得到针对每个应用程序150最优地制定的安全时间限制。在另一实施方式中，被入侵的会话时间限制可以被延长以用于进一步机器学习，这取决于终端用户的风险因素和配置。

[0037] 网络110表示客户端105和路由器115之间的通信路径。网络110可以包括有线网络、无线网络或有线网络和无线网络的组合。路由器110是在网络110和防火墙120之间路由数据包的网络设备。防火墙120可以过滤数据流量(traffic)，并且如果某些数据包不满足防火墙规则，则阻止这些数据包。负载均衡器125跨大量服务器130分发应用业务。

[0038] 在一个实施方式中，会话/连接管理器模型152可以被实现为软件指令、硬件逻辑或软件和硬件的组合。在一个实施方式中，会话/连接管理器模块152可以位于系统的其他地方，例如位于路由器115、防火墙120、负载均衡器125或后端服务器135中。在其他实施方式中，会话/连接管理器模块152的功能可以跨若干计算设备分布。

[0039] 现在转到图2，图2示出了根据实施方式的被划分为不同安全层的应用程序会话或连接。图2的会话/连接被分为四个安全层：安全层A202、安全层B 204、安全层C 206和安全层D 208。每个安全层表示随着会话/连接的长度增加而施加至会话/连接的更高级别的安全性。每个连续的安全层由应用程序会话/连接的持续时间达到不同的安全时间限制触发。每个安全层包括在其期间执行特定安全动作的若干安全阶段(即安全子层)。一般而言，会话/连接的状态具有不同的阶段，并且随着时间的推移，会话/连接的增加的安全性增加并且不同的规则和安全动作施加。

[0040] 安全层A202长达9秒。在安全层A202期间，最少数量的安全动作(例如，没有安全动作或几乎没有安全动作)被施加至会话/连接。在安全层A202期间通常不需要安全动作，原因是大多数正常的应用程序会话/连接预计在安全层A202结束之前终止。

[0041] 一旦会话/连接达到安全层A的9秒的时间限制，则安全级别从安全层A202提升到安全层B 204。安全层B 204长达9秒，并且在安全层B 204期间，基本的安全动作被施加至应用程序会话/连接。例如，在安全层B的阶段4期间，可以查找客户端设备105的IP地址，以确定地址是否是可疑地址。如果IP地址来自某些国家或如果IP地址是代理服务器或预定因素分析得到IP被标记为可疑，则该IP地址可能是可疑的。如果IP地址是可疑的，则安全级别可以跳过安全阶段5和安全阶段6中的任何安全动作而立即升级到安全层C 206。

[0042] 作为另一示例，在安全层B的阶段5期间，可以激活蜜罐安全传感器。蜜罐安全传感

器附接到包含假数据而不是真实数据的文件夹。具有假数据的文件夹可以具有附接到其上的安全传感器，安全传感器在文件夹中的文件被访问或打开文件夹时生成安全警报。例如，目录结构可以包括文件夹“/home/user1/”“/home/user2/”“/home/user3/”。真实数据仅存储在/home/user3/文件夹中，而不存储在/home/user1/或/home/user2/目录中。访问目录树的黑客不知道哪个目录包含真实数据，哪些目录包含假数据。因此，黑客可能会在会话/连接期间打开蜜罐文件夹，并触发蜜罐安全传感器。

[0043] 一旦会话/连接达到安全层B 204的9秒的时间限制(即，从会话/连接开始18秒的时间限制)，则安全级别从安全层B 204提升到安全层C 206。安全层C 206长达9秒，并且在安全层C 206期间将中级安全动作施加至应用程序会话/连接。例如，在安全层C 206的阶段7期间，应用程序会话/连接可以与其他应用程序会话隔离。稍后将参照图4和图5说明会话/连接隔离。

[0044] 作为另一示例，在安全层C 206的阶段8期间，可以对应用程序会话/连接的数据包执行深度数据包检查，以确定数据包是否是可疑的。如果确定数据包包括协议异常、SQL注入或者是畸形数据包，则数据包可能是可疑的。

[0045] 作为另一示例，在安全层C的阶段9期间，可以向其他网络设备(例如，路由器115、防火墙120或负载均衡器125)通知高风险会话。然后，其他网络设备可以发起其自身针对高风险会话的数据分析，并将该信息提供回至会话/连接管理器模块152。

[0046] 一旦会话/连接达到安全层C 206的9秒的时间限制(即，从会话/连接开始的27秒的时间限制)，则安全级别从安全层C 206提升到安全层D 208。安全层D 208长达9秒，并且在安全层D 208期间高级的安全动作被施加至应用程序会话/连接。例如，在安全层C 206的阶段10期间，可以遏制应用程序会话/连接，这会切断对真实数据的访问，只允许对假数据的访问。在安全层206的阶段11期间，可以执行发出警报、跟踪和记录。发出警报涉及例如通过电子邮件或SMS文本向网络管理员通知潜在的被入侵的会话。跟踪涉及跟踪应用程序会话期间执行的动作流，例如在应用程序会话期间访问文件目录的顺序。记录涉及存储跟踪期间捕获的数据，供以后由第三方工具进行离线分析以用于进一步调查。会话/连接也可以在阶段12结束时终止。

[0047] 在图2中，安全层和阶段都被示出为具有相同的持续时间。在其他实施方式中，安全层和阶段可具有不同的持续时间。在图2中示出了对于一些安全阶段的仅一些安全动作，但是现在在图2中示出的其他安全动作也可以在其他安全阶段期间执行。此外，与图2所示的相比，安全动作可以以不同的顺序和在不同的安全阶段期间来施加。

[0048] 另外，根据时间将安全性分为安全层并不一定防止会话/连接管理器模块152一直以高安全性运行。可以在不同的安全层202、204、206和208期间简单地施加不同组的安全规则。这防止误报，同时还允许计算资源集中于被入侵的会话/连接(其通常比非入侵会话/连接持续更长)。例如，安全层B 204还可以包括应用深度数据包检查的一组规则，但是仅当IP查找指示IP是可疑IP时才如此。

[0049] 图3是根据实施方式的划分成不同安全层的不同应用程序的应用程序会话/连接的示图。安全层的长度根据应用程序的类型而变化。对于信用卡处理应用程序150A，安全层可以长达9秒，并且每个安全阶段长达3秒。对于网络应用程序150B，安全层可以长达90秒，并且每个安全阶段长达30秒。对于网上银行应用程序150C，安全层可以长达9分钟，并且每

个安全阶段长达3分钟。

[0050] 参考信用卡示例，正常运行的信用卡处理应用程序150A通常将在5-10秒内处理交易，并通过5-10秒给予被批准或被拒绝的信用答案。本公开的实施方式剖析了平均信用卡交易的应用程序150A，并且根据平均信用卡交易时间计算出系统的基于时间的会话/连接时间限制。

[0051] 无论应用程序如何，在安全层中执行的安全动作可以跨应用程序相同。例如，对于所有三个应用程序，可以在安全层B 204期间进行IP查找。

[0052] 图4是示出根据实施方式的应用程序会话的隔离的示图。图5是示出根据另一实施方式的应用程序会话的隔离的示图。图4和图5都示出了来自图2的阶段7的会话/连接隔离安全动作。

[0053] 图4的会话/连接隔离通过在原始服务器上维护高风险会话/连接并且允许与服务器130A建立的其他会话/连接完成同时防止与该服务器130A的应用程序150建立任何新的会话/连接来进行。最初，存在与应用程序150建立的六个会话S1-S6，以及对应的连接C1-C6。然后确定会话S3已经打开了异常长的时间段，并且应该被隔离。为了隔离会话S3，允许会话S1、S2、S4、S5和S6完成。然而，不允许与服务器130A建立新的会话。最终，会话S3是与服务器130A的应用程序150建立的唯一会话，从而使会话S3和连接C3隔离。

[0054] 可替选地，为了隔离高风险会话S3，可以将其他会话(S1、S2、S4、S5、S6)从前端服务器130A移动到另一前端服务器130B，以防止数据被较高风险会话S3或连接危及。较高风险会话时间超出通常允许的时间，并对会话采取进一步的安全动作：对其进行分析处理，记录数据包，启动更深入的监测，连接/会话以完整的源数据终止以跟踪和追溯已经发生或正在发生的情况。动态访问控制列表(ACL)被放置在适当位置以用于阻止高风险会话S3执行任何类型的广泛搜索、扫描或下载较大的数据集。与数据库140的连接也可以根据会话的风险因素而被全部去除或限制。还可以记录与会话S3相关联的IP地址，并且客户端105可以被强制重新连接。第二次建立会话S3，会话/连接管理器模块152处于完全记录模式，以记录黑客会话S3的活动。黑客会话S3也可以被操纵以显示虚假的数据，以便在黑客实际没有找到数据时欺骗黑客陷入以为他已经找到了数据。后端数据库140也可以是真实的或被假数据库替代。

[0055] 图5的会话/连接隔离通过在服务器之间移动会话/连接来进行。最初，存在与前端服务器A 130A上的应用程序150建立的六个会话S1-S6和对应的连接C1-C6。然后确定会话S3已经打开了异常长的时间段并且应该被隔离。为了隔离会话S3，将会话S3和连接C3从前端服务器A 130A移动到不同的前端服务器B 130B。剩余的会话S1、S2、S4、S5和S6以及连接C1、C2、C4、C5和C6不受影响，并保留在前端服务器130A上。

[0056] 如图5所示，根据会话的时间，会话S3和连接C3的状态可以通过进行会话跳(session hop)或镜像来移动到另一服务器B 130B。上游设备(例如，路由器115、防火墙120、负载均衡器125)也被通知移动。这考虑到完全会话/连接迁移而没有断开用户会话/连接或者用户检测完全状态移动发生。如果在这种情况下黑客已经连接到前端服务器130A并且上传了远程脚本来危及服务器130A，则会话/连接跳将使改变后的应用程序位(application bit)保留在先前的服务器130A上，并且黑客会话/连接将或会被防止运作。会话/连接跳或故障转移可以开始基于跳生成警报，并且还具有多级状态改变。

[0057] 另外，前端服务器B 130B可以是专用安全服务器。专用安全服务器包括实时记录每个会话/连接数据包的能力，并且使得能够回放数据包以用于分析黑客如何进入系统，如上所述。

[0058] 图6是根据实施方式的来自图1的会话/连接管理器模块152的框图。会话/连接管理器模块152包括会话/连接监测模块605、应用程序剖析器模块610、安全级别提升模块615、安全动作模块620和时间限制确定模块625。在一个实施方式中，每个模块被实现为存储在计算机可读介质上的软件指令。

[0059] 会话/连接监测模块605监测应用程序150或网络业务，或者检测何时在任何客户端105和任何应用程序150之间建立新的应用程序会话/连接。一旦检测到新的应用程序会话/连接，则会话/连接监测模块605保持指示会话持续时间的会话/连接的会话/连接计数器。为每个会话/连接保持单独的会话/连接计数器，以便可以单独地跟踪会话/连接的持续时间。在任何给定时间，会话/连接监测模块605可以监测多个应用程序150的多个会话/连接。会话/连接监测模块605还可以识别针对其建立应用程序会话/连接的应用程序150的类型。

[0060] 应用程序剖析器模块610实现学习过程以捕获会话/连接的持续时间并且为应用程序安全简档154生成会话/连接持续时间数据。在一个实施方式中，应用程序剖析器模块610捕获应用程序150的会话/连接的会话/连接持续时间。处理会话/连接持续时间以生成应用程序150的会话/连接持续时间数据。会话/连接持续时间数据的示例包括：(1)应用程序会话/连接的最短观测持续时间，(2)应用程序会话/连接的最高观测持续时间，(3)应用程序会话/连接的平均观测持续时间，(4)应用程序会话/连接的实际持续时间，以及任何其他相关持续时间数据。然后将会话/连接持续时间数据存储到应用程序150的应用程序安全简档中。为不同的应用程序150重复该过程，以便每个应用程序150都自己独特的应用程序安全简档。

[0061] 应用程序剖析器模块610还可以捕获指示会话/连接是否被认为被入侵的入侵状态信息，其被存储在与会话/连接持续时间相关联的应用程序安全简档中。例如，如果黑客已经触发了系统内的蜜罐或其他安全传感器已经被触发，则认为会话/连接被入侵。

[0062] 时间限制确定模块625访问应用程序安全简档中的会话/连接持续时间数据，并使用该数据来确定将一个安全层与下一个安全层分开的安全时间限制。应用程序的安全时间限制仅从该应用程序的会话/连接持续时间数据导出。因此，应用程序A 150A的安全时间限制、应用程序B 150B的安全时间限制以及应用程序C 150C的安全时间限制将均不同。

[0063] 可以使用预先确定的数学公式从先前捕获的会话/连接持续时间数据导出安全时间限制。从会话持续时间数据计算会话的安全时间限制，并从连接持续时间数据计算连接的安全时间限制。例如，应用程序的会话的安全时间限制可以被计算为应用程序会话的平均持续时间的倍数(例如，2倍、6倍、8倍、10倍)。作为另一示例，应用程序的会话的时间限制可以被计算为应用程序会话的最长观测会话持续时间的倍数(例如，1倍、2倍、3倍、4倍)。因此，每种类型的应用程序150将具有最好地反映该特定应用程序的会话/连接特性的安全时间限制。

[0064] 时间限制确定模块620还可以确定使用类似过程将一个安全级与另一安全级分隔的时间限制。黑客状态信息还可以用于了解正常会话/持续时间的持续时间如何不同于被

入侵的会话/连接，这继而用于安全时间限制的设置。

[0065] 安全级别提升模块210控制从一个安全层到下一个安全层的提升。对于给定会话，安全级别提升模块210将会话/连接持续时间与为该会话建立的时间限制进行比较。一旦比较指示会话/连接持续时间已经达到相应的时间限制，则安全级别提升模块210将安全层提升到更高的安全层。

[0066] 在一个实施方式中，应用程序会话/连接的持续时间是从应用程序会话的开始起测量的总体持续时间。每个安全层的时间限制也从应用程序会话的开始起进行测量。在另一实施方式中，应用程序会话/连接的持续时间可以是表示单个安全层内的应用程序会话/连接的持续时间的部分持续时间。时间限制也可以是各个安全层的最大时间限制。

[0067] 安全动作模块620执行或发起各种安全动作，以确保前端服务器130、后端服务器135和数据库140免受恶意会话入侵。如前所述，安全动作的示例是IP查找、激活蜜罐传感器、会话/连接隔离、深度数据包检查、遏制会话、安全警报、会话/连接跟踪和会话/连接记录。在每个安全层中不同的安全动作被执行，并根据会话/连接的持续时间达到时间限制被触发。在一些实施方式中，可以对加密的会话数据执行安全动作中的一个或更多个安全动作。

[0068] 在一个实施方式中，安全动作模块620可以通过向上游或下游设备发送安全发起请求来发起安全动作，然后使其他设备执行安全动作。例如，路由器115、防火墙120、负载均衡器120或后端服务器135可以包括执行由安全动作模块620激活的安全动作的功能。安全动作模块620还可以从其他设备接收具有安全动作的结果的通信。

[0069] 图7是根据实施方式的用于剖析应用程序会话的方法的流程图。该流程图可以表示会话/连接管理器模块152的操作。在一些实施方式中，流程图的步骤可以以不同于图中所示的顺序执行。

[0070] 在步骤702中，检测应用程序的应用程序会话/连接。在步骤704中，监测和捕获会话/连接的持续时间。在步骤706中，从捕获到的会话/连接持续时间生成会话/连接持续时间数据。会话/连接持续时间数据被存储到与应用程序相关联的应用程序安全简档中。在步骤708中，一旦足够的会话/连接持续时间数据可用于先前建立的会话/连接，则访问安全简档，并且从安全简档中的会话/连接持续时间数据确定安全时间限制。安全时间限制指示一个安全层与另一个安全层之间的时间边界。

[0071] 对于不同的应用程序(例如，150A、150B、150C)重复数次图7中的过程，以生成大量的应用程序安全简档和针对每个应用程序的不同的安全时间限制，上述安全时间限制将应用程序的安全划分为表示增加安全风险级别的不同的安全层。

[0072] 图8是根据实施方式的用于会话/连接划分安全性的方法的流程图。该流程图可以表示通常发生在图7的流程图之后的会话/连接管理器模块152的操作。在一些实施方式中，流程图的步骤可以以不同于图中所示的顺序执行。

[0073] 在步骤805中，检测在客户端105和应用程序150之间建立的应用程序会话/连接。在步骤810中，识别与应用程序会话/连接相对应的应用程序150。在步骤825中，监测应用程序会话/连接的持续时间。在步骤830中，随着应用程序会话/连接的持续时间达到针对该应用程序确定的安全时间限制，应用程序会话/连接的安全级别随时间而增加。步骤830可以划分成若干子步骤840-870。

[0074] 在步骤840中，最初将安全性设置为最低安全层，例如安全层A 202。在最低安全层A 202期间，执行由最低的一组安全规则定义的最小数量的安全动作。

[0075] 在步骤845中，将会话/连接持续时间与初始安全时间限制进行比较。在步骤850中，如果会话/连接持续时间已经达到初始安全时间限制，则安全性增加到安全层B 204。在安全层B 204期间，由一组基本安全规则定义的基本安全动作被触发并被施加至应用程序会话/连接。通过针对应用程序会话/连接执行基本安全动作来施加基本安全动作。

[0076] 在步骤855中，将会话/连接持续时间与基本安全时间限制进行比较。在步骤860中，如果会话/连接持续时间已经达到基本安全时间限制，则安全性增加到安全层C 206。在安全层C 206期间，由一组中级安全规则定义的中级安全动作被触发并被施加至应用程序会话/连接。通过针对应用程序会话/连接执行基本的中级安全动作来施加中级安全动作。

[0077] 在步骤865中，将会话/连接持续时间与中级安全时间限制进行比较。在步骤870中，如果会话/连接持续时间已经达到中级安全时间限制，则安全性增加到安全层D 208。在安全层D 208期间，由一组高级安全规则定义的高级安全动作被触发并被施加至应用程序会话/连接。通过针对应用程序会话/连接执行高级安全动作来施加高级安全动作。

[0078] 可以对客户端105中的任何客户端和应用程序150A、150B或150C中的任何应用程序之间建立的每个应用程序会话/连接重复图8所示的过程，由此提供针对每个应用程序150A、150B或150C制定的防御黑客的基于时间的安全性。

[0079] 本公开的实施方式可以具有以下优点。剖析应用程序会话/连接可以实现更多的智能来进行更好的安全决策。将应用程序会话/连接关联到安全层可以允许基于有更高启迪的安全和决策制定。加强相关数据的分析允许在问题转变为全网络危害之前及时做出反应和遏制。对用于与数据中心中的所有设备进行安全集成的应用程序进行剖析改进了对网络中的黑客控制进行遏制。以时间分段的会话/连接开启新的安全性分析层次。在黑客不得不反复入侵以访问平台时可以进行更深入的分析。系统被入侵地越多，传感器获取应用程序、OS或协议中的可以修补的漏洞的机会就越大。

[0080] 图9示出了根据一个实施方式的诸如防火墙115、路由器120、负载均衡器125、客户端设备105、前端服务器130或后端服务器135的计算设备的硬件架构。在一个实施方式中，计算设备是包括组件(诸如通过总线901彼此交换数据和控制信号的处理器902、存储器903、存储模块904、输入模块(例如，键盘、鼠标等)906、显示模块907和通信接口905)的计算机。存储模块904被实现为一个或更多个非暂态计算机可读存储介质(例如，硬盘或固态驱动器)，并且存储软件指令940(例如模块)，软件指令940由处理器902结合存储器903执行以实现本文中所述的安全特征。软件指令的示例可以是软件代码或程序代码。操作系统软件和其他应用软件也可以存储在存储模块904中以在处理器902上运行。

[0081] 在阅读本公开后，本领域技术人员可以理解用于会话/连接划分安全性的另外的替代设计。因此，虽然已经示出和描述了本公开的特定实施方式和应用，但是应当理解，本公开不限于本文公开的精确构造和组件。在不脱离如在所附权利要求书中所限定的本公开的精神和范围的情况下，可以在本文中的本公开的方法和装置的布置、操作和细节上作出可能对本领域技术人员明显的各种修改、改变和变型。

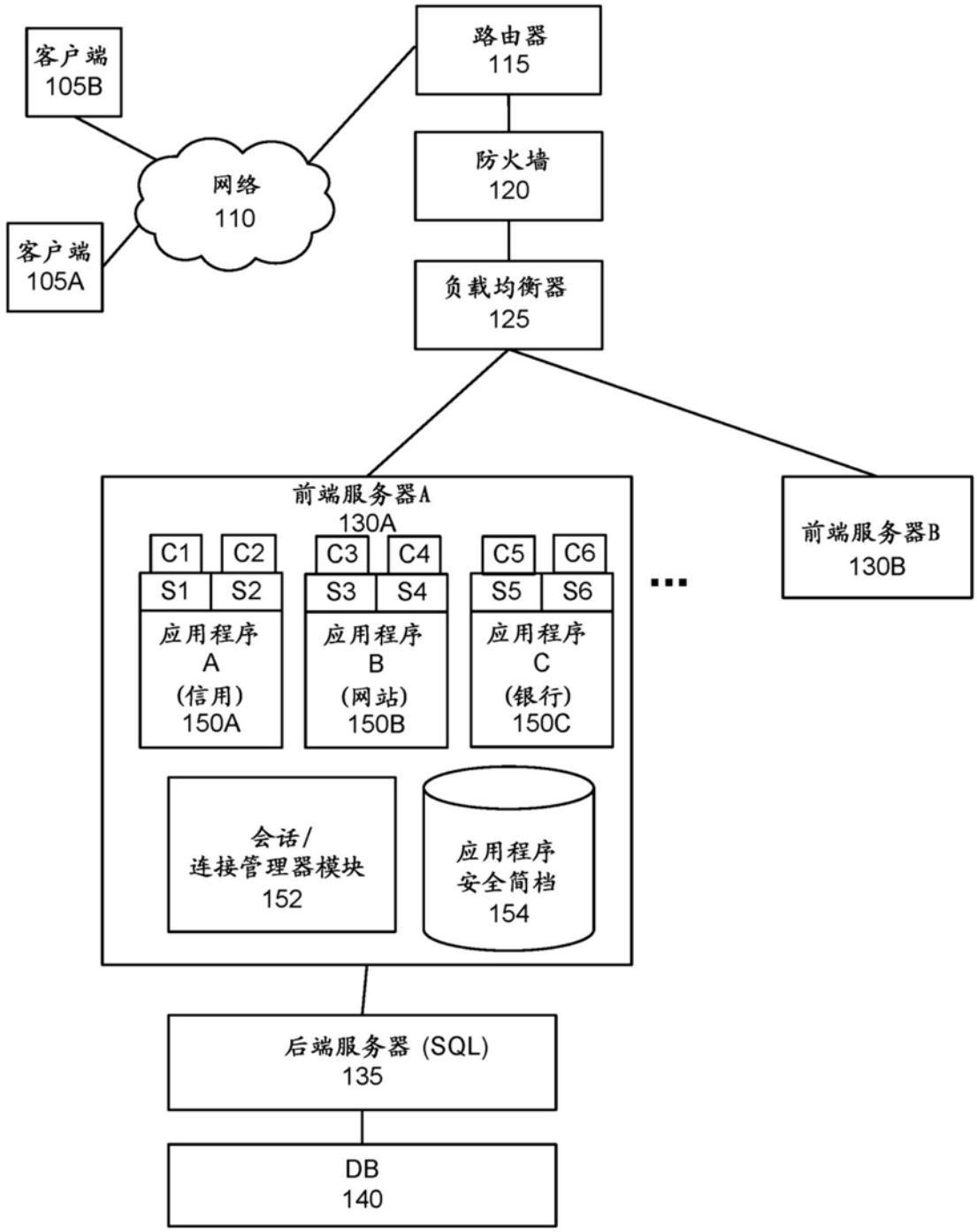

客户端
105B
客户端
105A
网络
110
路由器
115
防火墙
120
负载均衡器
125
前端服务器A
130A
C1
C2
C3
C4
C5
C6
S1
S2
S3
S4
S5
S6
应用程序
A
(信用)
150A
应用程序
B
(网站)
150B
应用程序
C
(银行)
150C
会话/
连接管理器模块
152
应用程序
安全简档
154
前端服务器B
130B
后端服务器 (SQL)
135
DB
140

图1

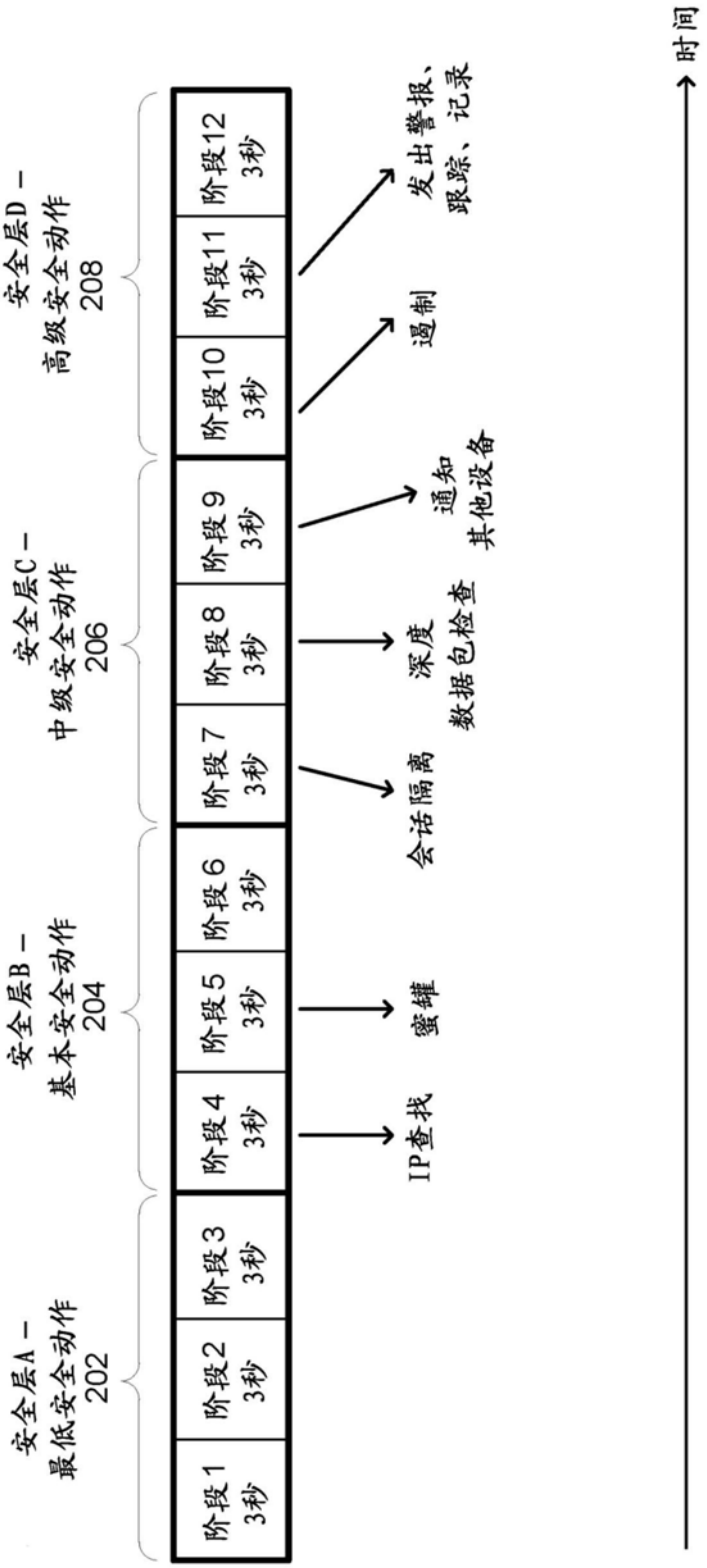

安全层A－
最低安全动作
202
安全层B－
基本安全动作
204
安全层C－
中级安全动作
206
安全层D－
高级安全动作
208
阶段1 3秒
阶段2 3秒
阶段3 3秒
阶段4 3秒
阶段5 3秒
阶段6 3秒
阶段7 3秒
阶段8 3秒
阶段9 3秒
阶段10 3秒
阶段11 3秒
阶段12 3秒
IP查找
蜜罐
会话隔离
深度数据包检查
通知其他设备
遏制
发出警报、跟踪、记录
时间

图2

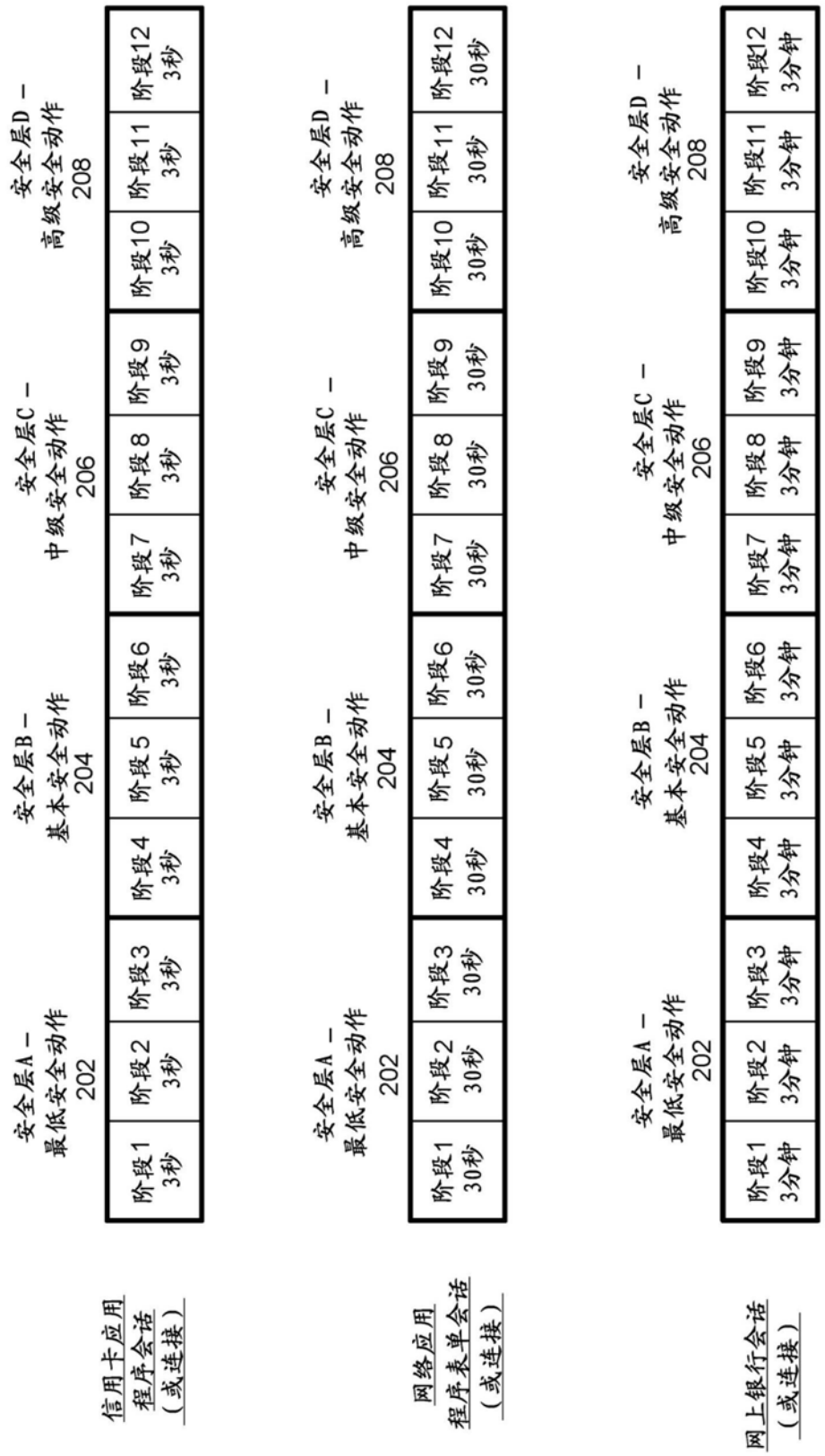

信用卡应用程序会话（或连接）
安全层A－最低安全动作 202
安全层B－基本安全动作 204
安全层C－中级安全动作 206
安全层D－高级安全动作 208
阶段1 3秒
阶段2 3秒
阶段3 3秒
阶段4 3秒
阶段5 3秒
阶段6 3秒
阶段7 3秒
阶段8 3秒
阶段9 3秒
阶段10 3秒
阶段11 3秒
阶段12 3秒
网络应用程序表单会话（或连接）
安全层A－最低安全动作 202
安全层B－基本安全动作 204
安全层C－中级安全动作 206
安全层D－高级安全动作 208
阶段1 30秒
阶段2 30秒
阶段3 30秒
阶段4 30秒
阶段5 30秒
阶段6 30秒
阶段7 30秒
阶段8 30秒
阶段9 30秒
阶段10 30秒
阶段11 30秒
阶段12 30秒
网上银行会话（或连接）
安全层A－最低安全动作 202
安全层B－基本安全动作 204
安全层C－中级安全动作 206
安全层D－高级安全动作 208
阶段1 3分钟
阶段2 3分钟
阶段3 3分钟
阶段4 3分钟
阶段5 3分钟
阶段6 3分钟
阶段7 3分钟
阶段8 3分钟
阶段9 3分钟
阶段10 3分钟
阶段11 3分钟
阶段12 3分钟

图3

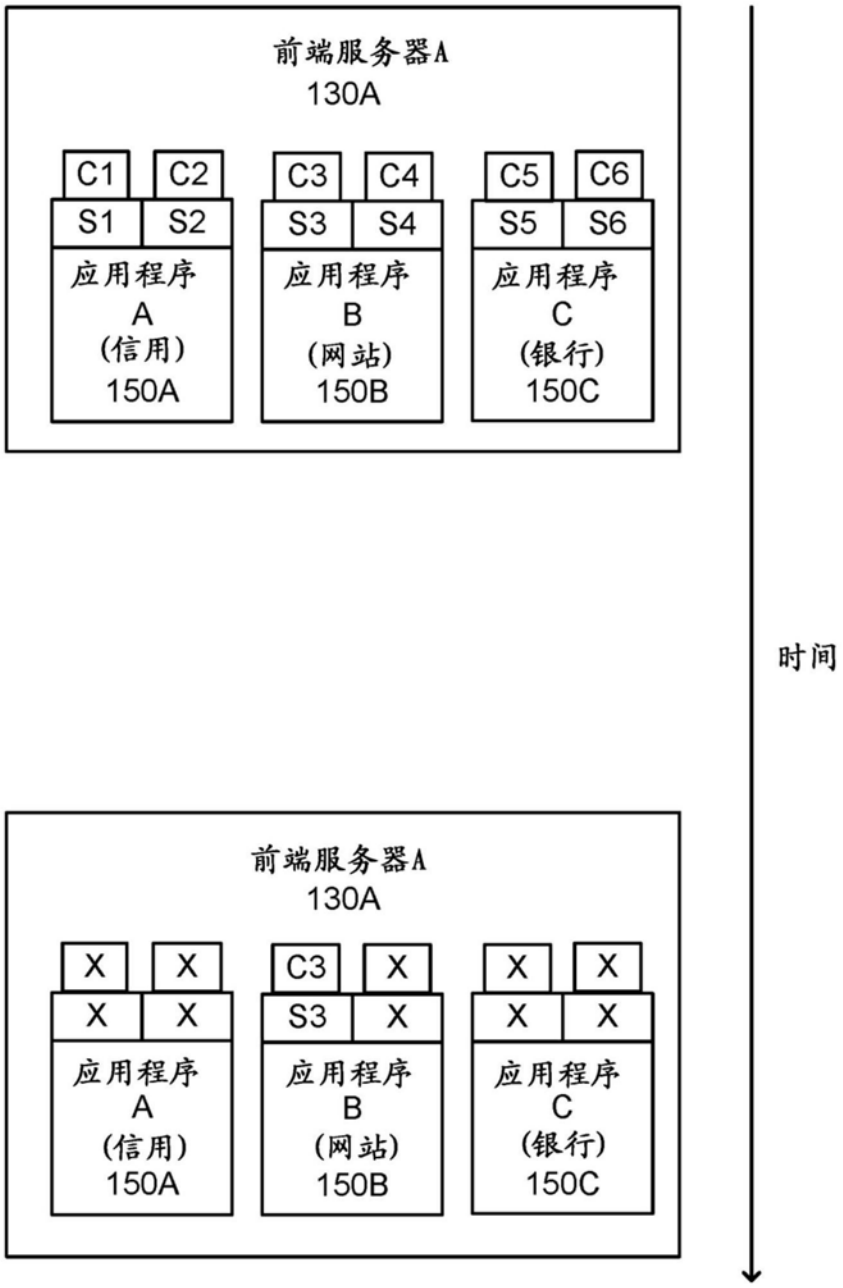

前端服务器A
130A
C1
C2
S1
S2
应用程序
A
(信用)
150A
C3
C4
S3
S4
应用程序
B
(网站)
150B
C5
C6
S5
S6
应用程序
C
(银行)
150C
时间
前端服务器A
130A
X
X
X
X
应用程序
A
(信用)
150A
C3
X
S3
X
应用程序
B
(网站)
150B
X
X
X
X
应用程序
C
(银行)
150C

图4

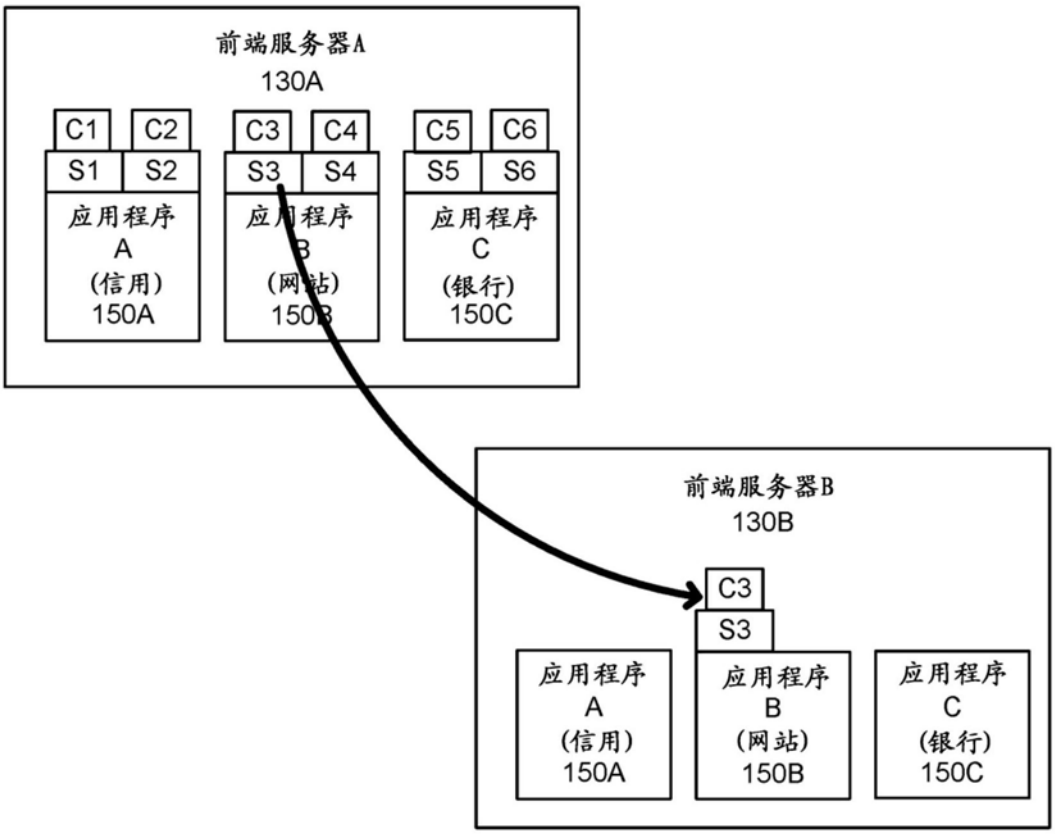

前端服务器A
130A
C1
C2
S1
S2
应用程序
A
(信用)
150A
C3
C4
S3
S4
应用程序
B
(网站)
150B
C5
C6
S5
S6
应用程序
C
(银行)
150C
前端服务器B
130B
C3
S3
应用程序
A
(信用)
150A
应用程序
B
(网站)
150B
应用程序
C
(银行)
150C

图5

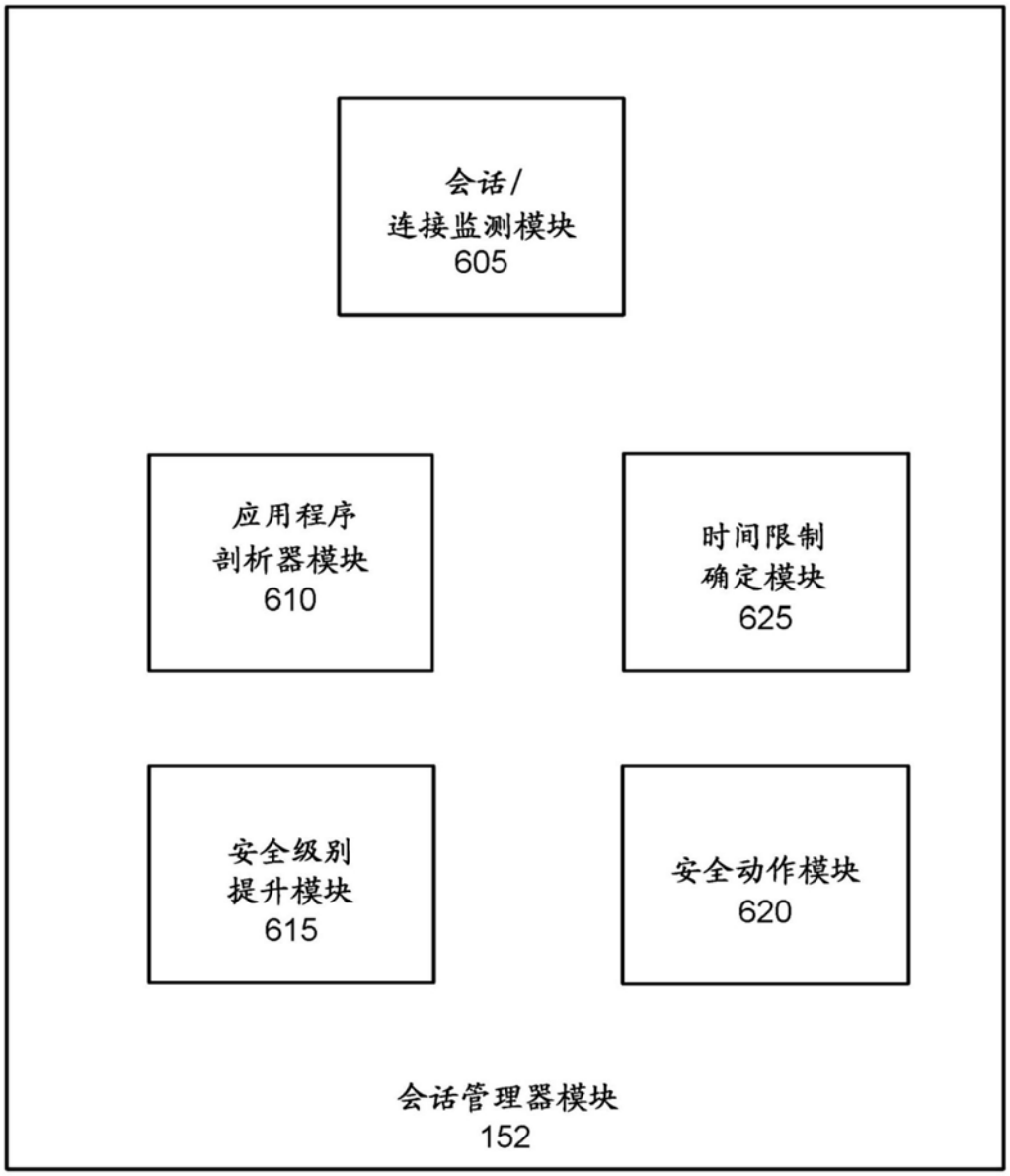

会话/
连接监测模块
605
应用程序
剖析器模块
610
时间限制
确定模块
625
安全级别
提升模块
615
安全动作模块
620
会话管理器模块
152

图6

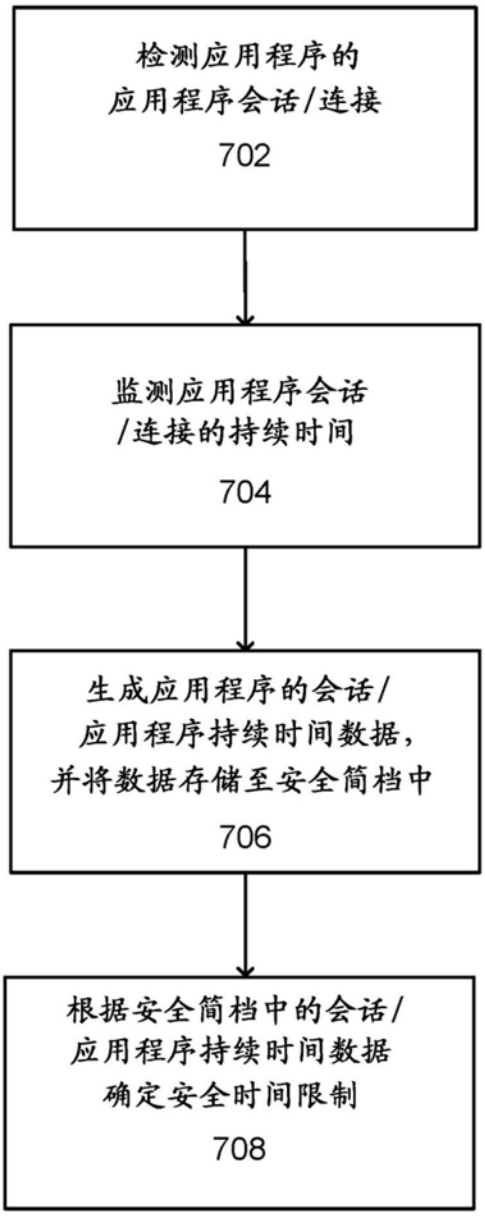

检测应用程序的
应用程序会话/连接
702
监测应用程序会话
/连接的持续时间
704
生成应用程序的会话/
应用程序持续时间数据，
并将数据存储至安全简档中
706
根据安全简档中的会话/
应用程序持续时间数据
确定安全时间限制
708

图7

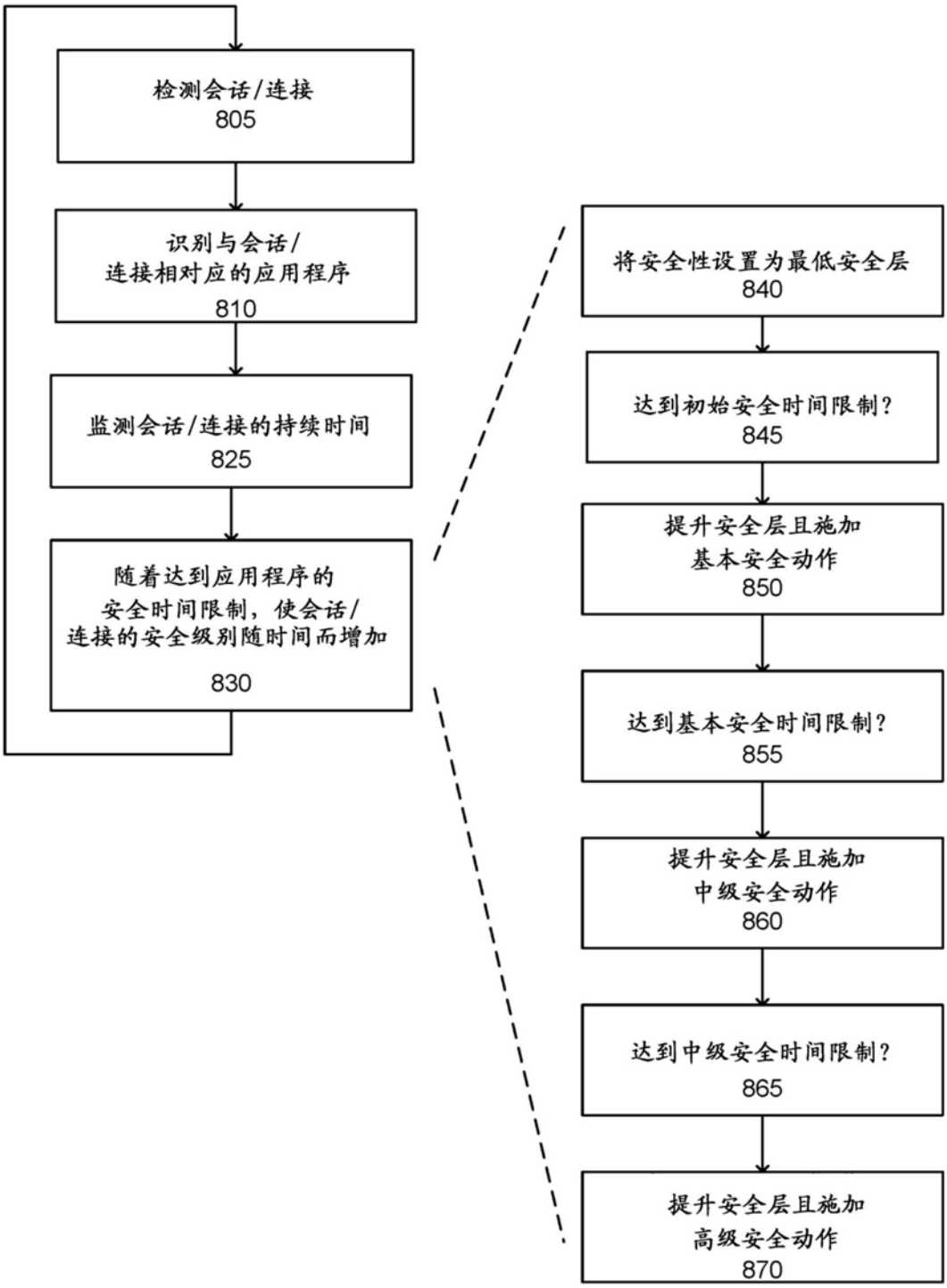

检测会话/连接
805
识别与会话/
连接相对应的应用程序
810
监测会话/连接的持续时间
825
随着达到应用程序的
安全时间限制，使会话/
连接的安全级别随时间而增加
830
将安全性设置为最低安全层
840
达到初始安全时间限制？
845
提升安全层且施加
基本安全动作
850
达到基本安全时间限制？
855
提升安全层且施加
中级安全动作
860
达到中级安全时间限制？
865
提升安全层且施加
高级安全动作
870

图8

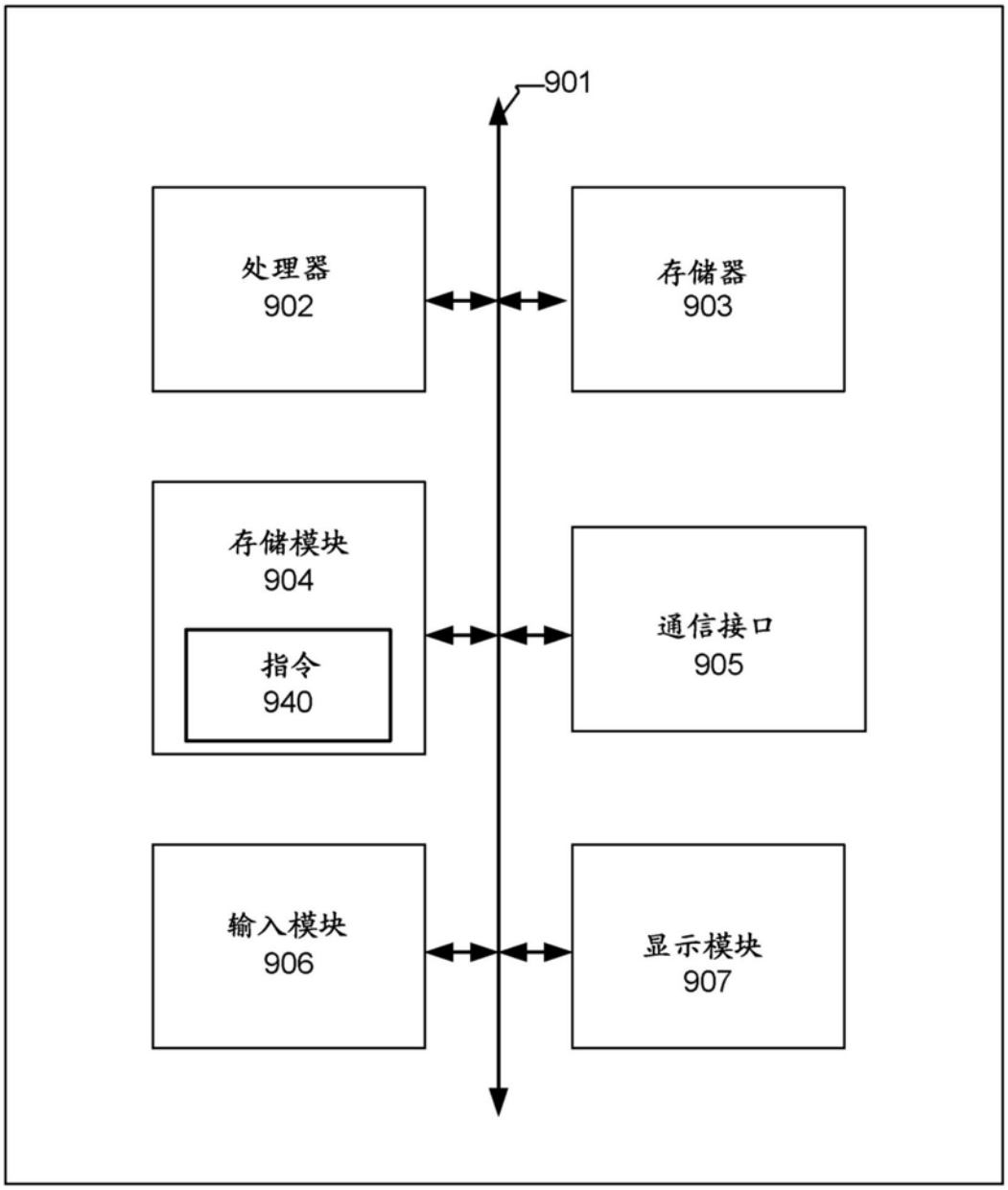


图9