(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 101669103 B
(45)授权公告日 2013.08.07

(21)申请号 200680045625.3
(22)申请日 2006.10.09
(30)优先权数据
11/249,846 2005.10.12 US
(85)PCT申请进入国家阶段日
2008.06.04
(86)PCT申请的申请数据
PCT/US2006/039376 2006.10.09
(87)PCT申请的公布数据
WO2007/047195 EN 2007.04.26
(73)专利权人 布卢姆伯格财政有限合伙公司
地址 美国纽约
(72)发明人 C·W·齐曼 J·W·胡克 D·杜莱
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 王英
(51)Int.Cl.
G06F 15/16(2006.01)
(56)对比文件
WO 98/19243 A2,1998.05.07, 全文.
US 5822435 A,1998.10.13, 说明书第5-9栏、附图1-6.
CN 1143436 A,1997.02.19, 全文.
US 2003/0200322 A1,2003.10.23, 全文.
CN 1478347 A,2004.02.25, 全文.
CN 1301437 A,2001.06.27, 全文.
审查员 林芳

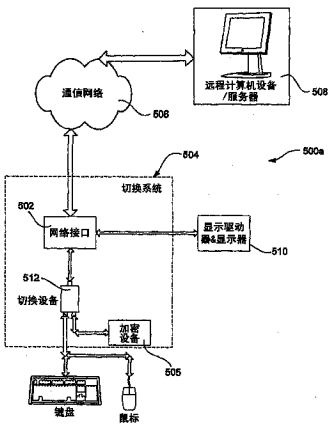
权利要求书5页 说明书16页 附图12页

(54)发明名称

提供安全数据传送的系统和方法

(57)摘要

本发明提供了一种系统和方法，其实施例包括基于来自由用户在本地计算机设备上启动的应用程序的鉴别而对输入数据进行加密。把由用户产生的该加密输入数据发送给与本地计算机设备有关的网络通信接口以便传送给远程计算机设备。在该远程计算机处，对所接收的输入数据进行解密，由此基于该解密输入数据，远程计算机产生与解密第一数据有关的加密响应数据。把加密响应数据从远程计算机发送给本地计算机，其中经由与该本地计算机有关的网络通信接口接收该加密响应数据并对其进行解密。该本地计算机在显示器上显示将该解密响应数据。



CN 101669103 B

1. 一种传递数据以便在第一计算机中使用的方法，包括：

在第一计算机处选择的第一通信模式中，所述第一计算机接收由与所述第一计算机相关联的一个或多个输入设备提供的数据，以便在所述第一计算机中执行的应用程序中由所述第一计算机使用，所述第一计算机在与所述第一计算机相关联的一个或多个显示设备上显示所接收的数据；

在所述第一计算机处选择的第二通信模式中，被配置为以安全的方式进行通信的第二计算机经由切换设备接收由所述一个或多个输入设备提供的数据，以便在所述第二计算机中执行的另一个应用程序中由所述第二计算机使用，而不由所述第一计算机处理或显示由所述一个或多个输入设备提供的所述数据；

在所述第二计算机中执行的所述另一个应用程序响应于由所述第二计算机接收的数据来生成数据；

所述切换设备以所述安全的方式接收响应数据，并且在所述第一计算机处选择了所述第二通信模式的情况下，将来自所述第二计算机的所述响应数据提供给所述第一计算机；以及

在所述第一计算机处选择了所述第二通信模式的情况下，所述第一计算机经由所述切换设备接收由所述第二计算机生成的所述响应数据，并且生成显示信息以用于在所述一个或多个显示设备上显示所接收的响应数据。

2. 如权利要求 1 所述的方法，

其中所述第一计算机响应用户激活在所述第一计算机中执行的所述应用程序而发送与被选中的所述第一通信模式相关联的第一指示；以及

其中所述第一计算机响应所述用户激活在所述第一计算机中执行的第二应用程序而发送与被选中的所述第二通信模式相关联的第二指示。

3. 如权利要求 1 所述的方法，

其中在所述第二计算机处接收所述数据包括利用所述第一计算机的网络接口在所述第二计算机处接收所述数据；以及

其中接收所述响应数据包括从所述第一计算机的所述网络接口接收来自所述第二计算机的对由所述一个或多个输入设备提供的所接收的数据的应答。

4. 如权利要求 1 所述的方法，其中在所述第二计算机处接收由所述一个或多个输入设备提供的所述数据包括：

对由所述一个或多个输入设备提供的所述数据进行加密；并且

在所述第二计算机处接收已加密数据。

5. 如权利要求 3 所述的方法，其中所接收的来自所述第二计算机的应答被加密，并且其中在所述第一计算机处接收所述应答包括：

对所接收的应答进行解密；并且

将已解密应答传送给所述第一计算机。

6. 一种利用加密设备在通信网络上提供数据通信的方法，该方法包括：

如果(a)选择安全通信模式：

将来自一个或多个输入设备的数据经由切换设备提供给所述加密设备；

所述加密设备对所述数据进行加密；

将已加密数据经由所述切换设备提供给与第一计算机相关联的接口，以传送给第二计算机；

发送所述已加密数据给所述第二计算机，而不由所述第一计算机处理或显示所述已加密数据或从所述一个或多个输入设备提供的数据；

在所述第二计算机处对所述已加密数据进行解密，并生成已加密响应数据；

将由所述第二计算机生成的所述已加密响应数据发送到与所述第一计算机相关联的所述接口；

所述接口将所述已加密响应数据经由所述切换设备提供给所述加密设备；

所述加密设备对所述已加密响应数据进行解密并提供已解密响应数据；

提供所述已解密响应数据给所述切换设备，在所述第一计算机处选择了所述安全通信模式的情况下，所述切换设备被配置为将来自所述第二计算机的响应数据提供给所述第一计算机；以及

所述第一计算机基于所述已解密响应数据进行操作；

否则(b)将来自所述一个或多个输入设备的数据提供给所述第一计算机而不进行加密，以便由所述第一计算机使用，其中所述第一计算机使由所述一个或多个输入设备提供的数据被显示在与所述第一计算机相关联的一个或多个显示设备上，并且在所述安全通信模式中，所述第一计算机使所述已解密响应数据被所述一个或多个显示设备进行显示。

7. 如权利要求 6 所述的方法，包括在所述安全通信模式中鉴别用户。

8. 如权利要求 7 所述的方法，其中所述鉴别包括启动应用程序，该应用程序提供所述加密设备和所述第一计算机之间的连接状态。

9. 如权利要求 8 所述的方法，其中所述鉴别包括响应所述应用程序产生的提示来扫描和检测与所述用户相关联的指纹图案，所述提示显示在与所述加密设备或所述第一计算机相关联的显示设备上。

10. 如权利要求 6 所述的方法，其中所述已解密响应数据包括所述第二计算机在与之相关联的显示设备上显示的显示数据。

11. 如权利要求 6 所述的方法，其中所述接口包括通用串行总线(USB)接口和网络接口。

12. 如权利要求 6 所述的方法，其中所述一个或多个输入设备包括键盘设备。

13. 如权利要求 6 所述的方法，其中所述一个或多个输入设备包括鼠标设备。

14. 如权利要求 6 所述的方法，其中所述一个或多个输入设备包括外围设备。

15. 一种利用耦合到第一计算机的加密设备在通信网络上在所述第一计算机和第二计算机之间提供数据通信的方法，该方法包括：

如果(a)与所述第一计算机相关联的第一应用程序是活动的：

将来自一个或多个输入设备的数据经由切换设备提供给所述加密设备；

所述加密设备对所述数据进行加密；

将已加密数据经由所述切换设备提供给与所述第一计算机相关联的接口，以传送给所述第二计算机；

发送所述已加密数据给所述第二计算机，而不由所述第一计算机处理或显示所述已加密数据或从所述一个或多个输入设备提供的数据；

在所述第二计算机处对所述已加密数据进行解密，并生成已加密响应数据；

将由所述第二计算机生成的所述已加密响应数据发送到与所述第一计算机相关联的所述接口；

所述接口提供所述已加密响应数据给所述加密设备；

所述加密设备对所述已加密响应数据进行解密；以及

所述加密设备提供已解密响应数据给所述切换设备，并且在与所述第一计算机相关联的所述第一应用程序是活动的情况下，所述切换设备被配置为将所述响应数据提供给在所述加密设备中操作的所述第一应用程序或者给所述第一计算机以由在所述第一计算机中操作的所述第一应用程序进行操作；

否则(b)将来自所述一个或多个输入设备的数据提供给所述第一计算机而不进行加密，以便在除了所述第一应用程序以外的程序中由所述第一计算机使用，其中所述第一计算机使由所述一个或多个输入设备提供的数据被显示在与所述第一计算机相关联的一个或多个显示设备上，并且当所述第一应用程序是活动的时，所述第一计算机使所述已解密响应数据被所述一个或多个显示设备进行显示。

16. 如权利要求 15 所述的方法，其中所述一个或多个输入设备包括键盘设备。

17. 如权利要求 15 所述的方法，其中所述一个或多个输入设备包括鼠标设备。

18. 如权利要求 15 所述的方法，其中所述一个或多个输入设备包括外围设备。

19. 如权利要求 15 所述的方法，其中所述第一应用程序驻留在所述第一计算机上，并且与驻留在所述第二计算机上的另一应用程序通信，其中所述另一应用程序生成所述响应数据，所述第一计算机处的所述第一应用程序在与所述第一计算机相关联的所述一个或多个显示设备上显示所述已解密响应数据。

20. 如权利要求 15 所述的方法，其中所述第一应用程序驻留在所述加密设备上，并且与另一应用程序通信，其中所述另一应用程序生成所述响应数据，所述加密设备处的所述第一应用程序在与所述第一计算机相关联的所述一个或多个显示设备上或在与所述加密设备相关联的显示设备上显示所述已解密响应数据。

21. 如权利要求 15 所述的方法，其中所述通信网络包括因特网。

22. 如权利要求 15 所述的方法，其中当所述第一应用程序提供的数据的焦点在与所述第一计算机相关联的显示设备上时，所述第一应用程序在所述第一计算机中是活动的。

23. 一种在第一计算机和第二计算机之间在通信网络上提供安全数据传送的系统，该系统包括：

切换设备；

加密设备；

第一计算机，被配置成运行第一应用程序和第二应用程序；

与所述第一计算机相关联的接口；以及

第二计算机；

所述切换设备用于从一个或多个输入设备接收数据并且可以被配置成当所述切换设备处于安全通信模式时将所述数据路由给所述加密设备以及当所述切换设备不处于安全通信模式时将所述数据路由给所述第一计算机；

所述第一计算机被配置成当所述切换设备不处于所述安全通信模式时从所述切换设

备接收所述数据并且在所述第一应用程序中使用所述数据；

所述加密设备被配置成当所述切换设备处于所述安全通信模式时从所述切换设备接收所述数据并对收到的数据进行加密；

与所述第一计算机相关联的所述接口被配置成当所述切换设备处于所述安全通信模式时接收已加密数据，并且在所述通信网络上将所述已加密数据发送给所述第二计算机，而不由所述第一计算机处理或显示所述已加密数据或从所述一个或多个输入设备接收的数据；

所述第二计算机被配置成接收所述已加密数据，自动生成已加密响应数据，并将所述已加密响应数据发送给所述接口；

所述接口被配置成提供由所述第二计算机生成的所述已加密响应数据给所述切换设备；

所述切换设备被配置成将所述已加密响应数据提供给所述加密设备；

所述加密设备被配置成对所述已加密响应数据进行解密并提供已解密响应数据给所述切换设备，在所述切换设备处于所述安全通信模式的情况下，所述切换设备被配置成将所述已解密响应数据提供给所述第一计算机；以及

所述第一计算机被配置成在所述第二应用程序中使用所述已解密响应数据并提供显示数据给与所述第一计算机相关联的一个或多个显示设备，并且所述第一计算机被配置成当所述切换设备不处于所述安全通信模式时将所述第一应用程序中使用的数据显示在与所述第一计算机相关联的所述一个或多个显示设备上。

24. 如权利要求 23 所述的系统，其中所述接口包括网络接口。

25. 如权利要求 23 所述的系统，还包括与和所述安全数据传送相关联的活动的应用程序通信的生物统计学鉴别设备，所述应用程序提示用户进行鉴别处理，所述加密设备被配置成仅在所述用户被鉴别后才对来自所述切换设备的数据进行加密。

26. 如权利要求 25 所述的系统，其中所述生物统计学鉴别设备包括指纹扫描仪。

27. 如权利要求 23 所述的系统，其中所述切换设备包括 USB 控制器，用于提供数据从所述一个或多个输入设备向所述第一计算机以及向所述加密设备的切换。

28. 一种给与服务器计算机通信的应用程序提供安全性的方法，该服务器计算机从与客户机计算机一起工作的输入设备接收输入，并且在与所述客户机计算机一起工作的一个或多个显示设备上显示信息，该方法包括：

如果(a)选择安全通信模式：

对通过所述输入设备输入的数据进行加密，而不提供输入的未经加密的数据给所述客户机计算机；

在网络上将已加密数据经由切换设备传送给所述服务器计算机，而不由所述客户机计算机处理或显示所述未经加密的数据或已加密数据，其中所述服务器计算机包括服务器应用程序；

在所述服务器计算机处对所述已加密数据进行解密；

所述服务器计算机使用所述服务器应用程序和已解密数据，并生成响应数据；

经由所述切换设备传送由所述服务器计算机生成的所述响应数据给所述客户机计算机，其中在选择了所述安全通信模式的情况下，所述切换设备将所述响应数据提供给所述

客户机计算机，以便由第一应用程序使用；以及

所述客户机计算机和所述第一应用程序使所述一个或多个显示设备显示所述响应数据；

或者(b)将通过所述输入设备输入的所述数据提供给所述客户机计算机而不进行加密以便在除了所述第一应用程序以外的应用程序中使用，其中所述客户机计算机使与所述客户机计算机一起工作的所述输入设备输入的数据被显示在所述一个或多个显示设备上。

29. 如权利要求 28 所述的方法，包括在所述服务器计算机处对所述响应数据进行加密并传送已加密响应数据给所述客户机计算机，并在所述客户机计算机处对所述已加密响应数据进行解密。

30. 如权利要求 29 所述的方法，其中传送给所述客户机计算机的已加密响应数据是独立于所述客户机计算机加以解密的，将这种已解密响应数据提供给所述客户机计算机，以在所述一个或多个显示设备上显示。

31. 如权利要求 28 所述的方法，其中所述输入设备包括键盘。

32. 如权利要求 28 所述的方法，其中所述输入设备包括指点设备。

33. 一种用于客户机计算机的方法，该客户机计算机与多个应用程序交互，并且给所述多个应用程序中的至少一个应用程序提供安全性，所述客户机计算机与服务器计算机通信并从输入设备接收输入，该方法包括：

如果在与所述客户机计算机相关联的一个或多个显示设备上在所述客户机计算机处所述至少一个应用程序包括处于焦点的窗：

对通过所述输入设备输入且与所述至少一个应用程序相关的数据进行加密，而不提供输入的未经加密的数据给所述客户机计算机；

在网络上将已加密数据经由切换设备传送给所述服务器计算机，而不由所述客户机计算机处理或显示所述未经加密的数据或已加密数据；

在所述服务器计算机处对所述已加密数据进行解密；

所述服务器计算机对已解密数据进行操作，并生成数据以由所述客户机计算机进行操作；

经由所述切换设备传送由所述服务器计算机生成的数据给所述客户机计算机，其中在所述窗处于焦点的情况下，所述切换设备将响应数据提供给所述客户机计算机；以及

所述客户机计算机对所生成的数据进行操作；

否则：

提供通过所述输入设备输入的数据给所述客户机计算机而不进行加密，以便由所述客户机计算机处置，其中所述客户机计算机使从所述输入设备接收的数据被显示在与所述客户机计算机相关联的一个或多个显示设备上，并且当所述窗处于焦点时，所述客户机计算机使所述已解密数据被所述一个或多个显示设备进行显示。

34. 如权利要求 33 所述的方法，包括在与所述输入设备和所述客户机计算机耦合并且在它们之间的设备中对与包括所述处于焦点的窗的所述至少一个应用程序相关的数据进行加密。

提供安全数据传送的系统和方法

[0001] 版权和法律声明

[0002] 本专利文档的部分说明书包含受版权保护的材料。如果出现在专利商标局的专利文件或者档案中，版权所有者不反对传真复制专利文档或专利说明书，但在其他方面保留其版权。

背景技术

[0003] 本发明通常涉及这样一种系统和方法，用于切换通信路径，以匹配期望的通信模式，具体而言，涉及基于是请求了安全还是非安全通信来提供安全或非安全通信路径。

发明内容

[0004] 根据本发明的一个实施例，提供一种传递数据的方法。这种方法包括：从一个或多个输入设备接收数据；如果从第一计算机收到已经选择第一通信模式的第一指示，就将所述数据传送给所述第一计算机。如果从所述第一计算机收到已经选择第二通信模式的第二指示，就将所述数据传送给第二计算机。

[0005] 根据本发明的另一个实施例，所述第一计算机响应用户激活所述第一计算机处的第一应用程序发送所述第一指示；所述第一计算机响应所述用户激活所述第一计算机处的第二应用程序发送所述第二指示。

[0006] 根据本发明的另一个实施例，如果从所述第一计算机收到所述第二指示，就从所述第二计算机接收对所传送的数据的应答。如果从所述第一计算机收到所述第二指示，就将收到的应答传送给所述第一计算机。

[0007] 根据本发明的另一个实施例，传送所述数据给第二计算机包括利用所述第一计算机的网络接口将所述数据传送给第二计算机；以及接收应答包括利用所述第一计算机的所述网络接口从所述第二计算机接收对所传送的输入数据的应答。

[0008] 根据本发明的另一个实施例，传送所述输入数据给第二计算机包括：对所述数据进行加密；并且将所述已加密数据传送给所述第二计算机。

[0009] 根据本发明的另一个实施例，从所述第二计算机收到的所述应答被加密。传送收到的所述应答给所述第一计算机包括：对收到的所述应答进行解密；并且将已经解密的收到的所述应答传送给所述第一计算机。

[0010] 根据本发明的另一个实施例，一种传递数据的系统，至少包括经过编程用于执行以下步骤的第一计算机：从一个或多个输入设备接收数据；如果从第二计算机收到已经选择第一通信模式的第一指示，就将所述数据传送给所述第二计算机。如果从所述第二计算机收到已经选择第二通信模式的第二指示，就将所述数据传送给第三计算机。

[0011] 根据本发明的另一个实施例，所述第二计算机响应用户激活所述第二计算机处的第一应用程序发送所述第一指示；以及所述第二计算机响应所述用户激活所述第二计算机处的第二应用程序发送所述第二指示。

[0012] 根据本发明的另一个实施例，所述第一计算机经过编程用于执行以下步骤：如果

从所述第二计算机收到所述第二指示，就从所述第三计算机接收对传送的所述数据的应答。如果从所述第二计算机收到所述第二指示，就将收到的应答传送给所述第二计算机。

[0013] 根据本发明的另一个实施例，所述第一计算机经过编程用于执行以下步骤：利用所述第二计算机的网络接口将所述数据传送给所述第三计算机。利用所述第二计算机的所述网络接口从所述第三计算机接收所传送的数据。

[0014] 根据本发明的另一个实施例，所述第一计算机经过编程使得传送所述数据给第三计算机包括：对所述数据进行加密；并且将所述已加密数据传送给所述第三计算机。

[0015] 根据本发明的另一个实施例，从所述第三计算机收到的所述应答被加密，并且所述第一计算机经过编程使得传送收到的所述应答给所述第二计算机包括：对收到的所述应答进行解密；并且将已经解密的收到的所述应答传送给所述第二计算机。

[0016] 根据本发明的另一个实施例，提供一种利用加密设备在通信网络上提供数据通信的方法。该方法包括：基于鉴别用户的所述加密设备对第一数据进行加密，其中将已加密第一数据从所述加密设备发送到与第一计算机相联系的接口，用于传送给第二计算机。在所述第二计算机处对所述已加密第一数据进行解密，根据所述已解密第一数据产生已加密第二数据。将产生的所述已加密第二数据发送到与所述第一计算机相联系的所述接口，用于传送给所述加密设备；并且在所述加密设备处对通过与所述第一计算机相联系的所述接口收到的被发送的所述已加密第二数据进行解密。所述第一计算机基于所述已解密第二数据进行操作。

[0017] 根据本发明的另一个实施例，鉴别所述用户包括运行应用程序开始鉴别过程。

[0018] 根据本发明的另一个实施例，所述鉴别过程包括运行的所述应用程序提供所述加密设备和所述第一计算机之间的连接状态。

[0019] 根据本发明的另一个实施例，所述鉴别过程包括在收到所述应用程序产生的提示时扫描和检测与所述用户相联系的指纹图案。

[0020] 根据本发明的另一个实施例，所述已解密第二数据包括响应所述第二计算机设备处理的所述第一数据所产生的显示数据。

[0021] 根据本发明的另一个实施例，所述接口包括通用串行总线 (USB) 接口和网络接口。

[0022] 根据本发明的另一个实施例，所述第一数据是由键盘设备、鼠标设备和 / 或外围设备产生的。

[0023] 根据本发明的另一个实施例，提供一种利用耦合到第一计算机的加密设备在通信网络上在所述第一和第二计算机之间提供数据通信的方法。该方法包括：基于与所述数据通信相联系的活动的应用程序在所述加密设备处对第一数据进行加密，其中将已加密第一数据从所述加密设备发送到与所述第一计算机相联系的接口，用于传送给所述第二计算机。在所述第二计算机处对所述已加密第一数据进行解密，根据所述已解密第一数据产生已加密第二数据；将产生的所述已加密第二数据发送到与所述第一计算机相联系的所述接口，用于传送给所述加密设备。在所述加密设备处对通过与所述第一计算机相联系的所述接口收到的被发送的所述已加密第二数据进行解密；其中所述加密设备提供所述已解密第二数据给所述第一计算机供所述第一计算机处置。

[0024] 根据本发明的另一个实施例，所述第一数据是由键盘设备、鼠标设备和 / 或外围

设备产生的。

[0025] 根据本发明的另一个实施例，所述应用程序驻留在所述第一计算机上，并且与驻留在所述第二计算机上的第二应用程序通信。所述第二应用程序产生所述第二数据，所述第一计算机上的所述应用程序显示所述已解密第二数据。

[0026] 根据本发明的另一个实施例，所述应用程序驻留在所述加密设备上，并且与第二应用程序通信，其中所述第二应用程序产生所述第二数据，所述加密设备处的所述应用程序显示所述已解密第二数据。

[0027] 根据本发明的另一个实施例，其中通信网络包括因特网。

[0028] 根据本发明的另一个实施例，对第一数据加密包括基于与所述应用程序相联系的焦点窗在所述加密设备处对第一数据进行加密。

[0029] 根据本发明的另一个实施例，提供一种在通信网络上在第一和第二计算机之间产生安全数据传送的安全系统。该系统包括：切换设备，用于从一个或多个输入设备接收第一数据；加密设备，用于从所述切换设备接收路由过来的所述第一数据，用于基于与所述安全数据传送相联系的活动的应用程序，对收到的所述第一数据进行加密；与所述第一计算机相联系的接口用于接收已加密的所述第一数据，用于在所述通信网络上传送给所述第二计算机，其中所述第二计算机接收所述已加密第一数据并产生已加密第二数据；以及与所述第一计算机相联系的显示器设备。在所述第二计算机处产生的所述已加密第二数据由所述接口从所述通信网络收到，并发送给所述切换设备进行路由，其中所述切换设备将所述已加密第二数据路由给所述加密设备，用于对所述已加密第二数据进行解密。所述切换设备将所述已解密第二数据从所述加密设备路由给所述第一计算机，用于在所述显示器设备上显示。

[0030] 根据本发明的另一个实施例，接口包括网络接口。

[0031] 根据本发明的另一个实施例，生物统计学鉴别设备与所述应用程序通信，所述应用程序提醒用户进行鉴别处理。所述加密设备在对所述输入数据进行加密之前对所述用户进行鉴别。

[0032] 根据本发明的另一个实施例，生物学鉴别设备包括指纹扫描仪。

[0033] 根据本发明的另一个实施例，所述切换设备包括 USB 控制器，用于在所述一个或多个输入设备、所述第一计算机和所述加密设备之间提供数据切换。

[0034] 根据本发明的另一个实施例，一种给应用程序提供安全性的方法，该应用程序与服务器计算机通信，该服务器计算机与客户机计算机一起工作，从输入设备接收输入，并且在显示器设备上显示信息，该显示器设备与所述客户机计算机一起工作。该方法包括：对数据进行加密，所述数据与所述应用程序相关，通过所述输入设备输入，而不提供未经加密的输入数据给所述客户机计算机。在网络上传送所述已加密数据给所述服务器计算机；对传送给所述服务器计算机的所述已加密数据进行解密。所述服务器计算机对所述已解密数据进行操作，并提供数据用于在所述客户机计算机上显示。传送所述服务器计算机提供的所述数据用于在所述客户机计算机的所述显示器设备上显示；在所述显示器设备上显示所述服务器计算机提供的传送的数据。

[0035] 根据本发明的另一个实施例，在将所述服务器计算机提供的数据传送给所述客户机计算机之前对这样的数据进行加密，在传送以后显示之前进行解密。在所述客户机计算

机的显示器设备上显示所述已解密数据。

[0036] 根据本发明的另一个实施例，传送给所述客户机计算机的已加密数据是独立于所述客户机计算机加以解密的，将这种已解密数据提供给所述客户机计算机在所述显示器设备上显示。

[0037] 根据本发明的另一个实施例，输入设备包括键盘和 / 或指点设备。

[0038] 根据本发明的另一个实施例，提供一种用于客户机计算机的方法，该客户机计算机与多个应用程序交互，并且给所述多个应用程序中的至少一个应用程序提供安全性，该至少一个应用程序与服务器计算机通信，该服务器计算机从与所述客户机计算机一起工作的输入设备接收输入。该方法包括：如果所述客户机计算机处的所述至少一个应用程序包括焦点窗：对数据进行加密，所述数据与所述至少一个应用程序相关，通过所述输入设备输入，而不提供未经加密的输入数据给所述客户机计算机。在网络上传送所述已加密数据给所述服务器计算机；对传送给所述服务器计算机的所述已加密数据进行解密。所述服务器计算机对所述已解密数据进行操作，并提供数据用于供所述客户机计算机进行操作。传送提供的所述数据给所述客户机计算机；以及所述客户机计算机对提供的数据进行操作。如果所述客户机计算机处的所述至少一个应用程序包括焦点窗：提供通过所述输入设备输入的数据给所述客户机计算机而不加密供所述客户机计算机处置。

[0039] 根据本发明的另一个实施例，在与所述输入设备和所述客户机计算机耦合的设备中对与选择的应用程序相关的数据加密。

[0040] 根据本发明的另一个实施例，当与所述至少一个活动应用程序相联系的所述窗处于焦点时，耦合所述键盘的输出到所述设备的输出，该设备耦合到所述客户机计算机，用于与所述至少一个活动应用程序操作。

[0041] 根据本发明的另一个实施例，当与至少一个活动应用程序相联系的所述窗处于焦点时，自动耦合所述键盘的所述输出到所述设备的所述输出，所述设备耦合到所述客户机计算机。

附图说明

[0042] 本发明被例示于附图的图形中，其仅意味着示范而不是限制，并且其中相同的参考标记是指相同或对应的部件。

[0043] 图 1 是举例说明根据本发明实施例的数据通信系统的框图；

[0044] 图 2 是举例说明根据本发明实施例的包括切换系统的数据通信系统的框图；

[0045] 图 3 是举例说明根据本发明实施例的数据通信系统的安全传送路径的示意图；

[0046] 图 4A-4B 是举例说明根据本发明实施例的在安全操作模式下操作切换系统的流程图；

[0047] 图 5、6、7 和 8 是举例说明了根据本发明实施例的一种方法的流程图，通过该方法数据通信系统可基于应用程序窗口聚焦来操作安全模式应用程序和切换系统；

[0048] 图 9 是举例说明根据本发明实施例的切换系统的组件的框图；

[0049] 图 10 是根据本发明实施例的 USB 控制器设备的框图；以及

[0050] 图 11A 和 11B 是举例说明根据本发明实施例的合并有切换系统的替换实施例的系统框图。

具体实施方式

[0051] 图 1 举例说明了根据本发明实施例的数据通信系统 10。数据通信系统 10 包括用户计算机 12、要访问的计算机 18（也称为“被访问计算机”）、网络 20 和切换系统 22。

[0052] 用户计算机 12 可以包括可由用户操作的任何计算机。在本发明的实施例中，用户计算机 12 还能够接收来自其他计算机的数据并根据来自其他计算机的数据采取动作。例如，用户计算机 12 可以包括 PC 机、工作站或 PDA，他们能够接收和显示从服务器中所接收的数据。与用户计算机 12 相关联的是用于向用户提供输出的一个或多个输出设备 14，例如显示设备或打印机。同样地，一个或多个数据输入设备 16，例如鼠标和 / 或键盘，可以通过切换系统 22 与用户计算机 12 进行通信。

[0053] 在本发明的一个实施例中，用户计算机 12 还包括向切换系统 22 指示期望多个通信模式中之一的功能。每种通信模式可以由例如不同的通信目的地（诸如通信接收端的不同计算机）来表征。例如，其中用户计算机 12 能够同时运行一个以上的应用程序，用户计算机 12 根据第一、第二或第三组应用程序中的一个应用程序是否是激活的来向切换系统 22 提供用于表示第一、第二或第三通信模式是所期望的通信模式的指示。例如，激活的应用程序包括正聚焦的应用程序窗口。

[0054] 被访问计算机 18 包括可与其他计算机进行通信的任何计算机。例如，被访问计算机 18 包括能够通过网络与客户机进行通信的计算机服务器。如果需要，被访问计算机 18 可以使用安全方式（例如加密和解密）与其他计算机进行通信。

[0055] 被访问计算机 18 可以通过网络 20 与切换系统 22 进行通信。此处使用的网络广泛包括任何通信路径，经由所述通信路径计算机系统可与包括但不限于下列中的一个或多个网络进行通信：私人的、专用电信线路、有线或无线的 LAN 和 WAN 以及因特网。

[0056] 此外，切换系统 22 与被访问计算机 18 进行通信所经由的网络包括用户计算机 12。例如，如图 2 所示和如以下的进一步描述，切换系统 22 可经由用户计算机 12 和网络与被访问计算机 18 进行通信，所述网络提供了用户计算机 12 和被访问计算机 18 之间的通信路径，例如网络 24。此处广泛使用的通信路径是指物理通信路径、逻辑通信路径或者其组合。

[0057] 切换系统 22 提供了输入设备 16 与用户计算机 12 之间和输入设备 16 与被访问计算机 18 之间的通信路径（经由网络 20）。(a) 基于期望多种通信模式中哪一种模式的指示，切换系统 22 的作用在于在这些通信路径之间动态地切换输入设备 16，以及 (b) 把数据从输入设备 16 传送给位于激活的通信路径的接收端处的计算机系统。

[0058] 如上所述，切换系统 22 从用户计算机 12 接收用于表示期望多个通信模式中哪一种模式的指示。例如，用户计算机 12 基于从第一组应用程序中激活的应用程序而向切换系统 22 发送用于表示期望第一通信模式的指示，当收到这个指示时，切换系统 22 使输入设备 16 与用户计算机 12 之间的通信路径被激活。其中用户计算机 12 基于从第二组应用程序中激活的应用程序而向切换系统 22 发送用于表示期望第二通信模式的指示，当收到这个指示时，切换系统 22 使输入设备 16 与被访问计算机 18 之间的通信路径被激活。

[0059] 根据本发明的一个实施例，在激活输入设备 16 和被访问计算机 18 之间的通信路径的通信模式下，切换系统 22 还被用作从被访问计算机 18 中接收数据并且把所接收的数据馈送给用户计算机 12。例如，在其中用户计算机 12 基于从第二组应用程序中激活的应用

程序而发送第二通信模式的指示的上述示例之后，切换系统 22 把数据从输入设备 16 传送到被访问计算机 18，所述被访问计算机 18 对数据进行处理并且向切换系统 22 发回应答。切换系统 22 之后可以向用户计算机 12 发送该应答，例如发送给第二组应用程序中激活的应用程序，以便操作，例如显示给用户。

[0060] 如果期望，切换系统 22 可以在安全模式（例如利用加密和解密）下与其他计算机系统进行通信。因而，在上述示例中，切换系统 22 可以在把来自输入设备 16 的数据通过网络 20 发送给被访问计算机 18 之前，对来自输入设备 16 的数据进行加密。被访问计算机 18 然后对数据进行解密、处理，并把加密应答传送回切换系统 22。然后切换系统 22 可在向用户计算机 12 发送这个应答之前解密该应答。

[0061] 切换系统 22 可以包括能够实现上述功能的任何计算机系统。这些功能可以通过硬件、软件或者其组合实现。下面来进一步描述切换系统 22 不同实施例的示例以及可执行上述功能的组件。

[0062] 尽管图 1 和 2 仅显示了一个被访问计算机 18，但是任意数量的这种系统均可包含在本发明之内，其中切换系统 22 以上述类似的方式在通信路径之间把输入设备 16 动态地切换到每条通信路径。例如，五种通信模式可以分别对应于输入设备 16 与五个不同的通信目的地之间的通信路径，例如用户计算机 12 和四个不同的被访问计算机。

[0063] 此处使用的计算机是广泛指计算机硬件和软件或者仅指计算机软件。例如，上述四个被访问计算机可以全部是共同驻留于相同硬件平台上的单独的服务器应用程序。

[0064] 如上所述的本发明的实施例在其中用户希望访问一台计算机（例如被访问计算机 18），但是该用户的计算机（例如用户计算机 12）是一台不可靠的计算机的情况下是有益的。例如，用户的计算机对于外部攻击（例如来自病毒的）而言容易损坏，其中输入到计算机的数据（例如击键）可能被监控并被传送到第三方。在这种情况下，根据如上所述的本发明的实施例，当用户试图通过例如用户计算机 12 上的相应客户机应用程序来访问被访问计算机 18 时，切换系统 22 可以把数据从输入设备 16 引导到被访问计算机 18 处以供处理，并且把从被访问计算机 18 中接收的应答发送给用户计算机 12 上的客户机应用程序以供操作，例如显示给用户。因此，在这种情况下，要由用户输入到被访问计算机的数据不通过用户的计算机来发送，并且不容易受到如上所述的攻击。

[0065] 如上所述，被访问计算机 18 通过安全方式（例如采用加密和解密）与其他计算机进行通信。例如，被访问计算机 18 和用户计算机 12 可采用传送层安全 (TLS) 协议来安全地通信。

[0066] 图 3 举例说明了一种根据本发明实施例的，用以提供安全通信的数据通信系统。安全的数据通信系统 100 包括如前所述的切换系统 102。如图 3 的实施例所示，切换系统 102 包括数据切换设备 104 和加密设备 106。安全通信系统 100 还包括如上所述的用户计算机 108 和被访问计算机 110。如图 3 所示，用户计算机 108 经由网络 112 与被访问计算机 110 进行通信。在图 3 的实施例中，显示设备 114 与用户计算机 108 以及例如鼠标 116 和 / 或键盘 118 之类的一个或多个数据输入设备相关联。根据图 3 的实施例，被访问计算机 110 包括一个或多个服务器计算机。

[0067] 另外，可以利用提供输入数据的其他设备。例如，除键盘 116 和鼠标 118 之外，或者代替键盘 116 和鼠标 118，可以使用触摸屏显示设备、声音识别系统和 / 或能够提供输入

数据的其他外设来输入数据。

[0068] 系统 100 的各种组件之间的数据通信被指定为沿着通信路径 P1、P2、P3、P4 和 P5 来进行，其中每一个通信路径包括如前所述的物理或逻辑通信路径或者其组合。每个路径可以采用不同的通信介质，例如光纤介质，无线装置（例如射频和红外）或者基于电缆的数据传送介质。

[0069] 根据图 3 的实施例，路径 P2 是包括至少两个逻辑通信路径（例如 P2a 和 P2b）的物理通信路径。如以下的进一步描述，路径 P2a 在切换系统 102 和用户计算机 108 之间承载数据以便进行本地处理（例如，由用户计算机 108 上运行的程序）。如以下的进一步描述，路径 P2b 在切换系统 102 和用户计算机 108 之间承载数据以便传送给被访问计算机 110 或者从被访问计算机 110 中接收（例如，使用用户计算机 108 的网络接口以便在网络 112 上进行通信）。

[0070] 从鼠标 116 和键盘 118 所接收的输入数据沿着路径 P1 被发送给数据切换设备 104。切换设备 104 判断是否应沿着路径 P3 把数据切换给加密设备 106。如果建立了安全模式通信会话，则经由路径 P1 和 P3 把输入数据发送给加密设备 106。换句话说，如果不需要安全模式通信会话，则把沿着路径 P1 的输入数据沿着路径 P2a 切换给用户计算机 108 以便进行本地处理（例如由用户计算机 108 上运行的程序）。

[0071] 由用户计算机 108 产生的显示信息被显示在显示设备 114 上。该显示信息可以作为用户计算机 108 上运行的程序的结果或者作为由用户计算机 108 通过网络 112 从被访问计算机 110 中接收的数据信息的结果而产生。

[0072] 数据可以在用户计算机 108 和被访问计算机 110 之间被发送与接收。例如，可以沿着路径 P1 和 P3 把已加密输入数据发送给加密设备 106。在加密之后，通过路径 P3 和 P2b 把已加密数据发送给用户计算机 108，其中经由用户计算机 108（未示出）的网络接口沿着路径 P4 和 P5 把已加密数据发送给被访问计算机 110。不由用户计算机 108 对已加密数据进行本地处理是一种安全的运行方式。相反，将其发送给被访问计算机 110 来处理，由此被访问计算机 110 可以仅在解密的基础上对该加密数据进行处理。

[0073] 换句话说，例如可以通过路径 P1 和 P2a 把未加密输入数据发送给用户计算机 108 来进行本地处理。继用户计算机 108 对未加密输入数据进行处理之后，未加密数据可以由用户计算机 108 上运行的程序来产生，并且通过用户计算机 108 的网络接口沿着路径 P4 和 P5 而发送给被访问计算机 110。同样，在用户计算机 108 处本地处理的未加密输入数据可以被显示在显示设备 114 上。输入数据由计算机 108 直接进行处理是一种非安全的运行方式。

[0074] 基于通过网络 112 进行安全数据传送的用户需求和需要，由被访问计算机 110 产生的数据可以被加密或者不被加密。例如，要给用户计算机 108 上运行的程序的，从被访问计算机 110 中收到的未加密数据，可以由用户计算机 108 借助于作为数据传送目标的程序来进行本地处理。然后把从被访问计算机 110 中收到的，且由用户计算机 108 来进行本地处理的该未加密数据在显示设备 114 上显示给用户。换句话说，例如，由被访问计算机 110 产生的，以便由用户计算机 108 作最后处理的已加密数据可以通过路径 P5 和 P4 而被发送给用户计算机 108。将已加密数据传送给切换系统 102。从而，当由用户计算机 108 的网络接口接收已加密数据时，沿着路径 P26 把已加密数据传送给切换系统 102 和切换设备 104。

在切换设备 104，已加密数据被接收并且通过路径 P3 被发送给加密设备 106，在加密设备中对已加密数据进行解密。继解密处理之后，通过路径 P3 把已解密数据发送给切换设备 104，在切换设备 104 处通过路径 P2a 把已解密数据发送给用户计算机 108。然后为了在显示器 114 上进行显示的目的而在用户计算机 108 处对已解密数据进行本地处理。

[0075] 图 4A 和 4B 举例说明了根据本发明实施例的加密操作模式的操作流程图。结合图 3 所示的安全数据通信系统 100 对这些流程图进行描述。在步骤 202 处，加密设备 106 经由连接器、无线链路或者其他适当的耦合 / 通信模式（未显示）而连接到切换设备 104 以组成切换系统 102。如果加密设备 106 和切换设备 104 被预先集成在单个单元之内，也可以不需要上述连接。切换系统 102 可以通过通用串行总线 (USB) 连接和 / 或其它连接介质和协议而连接于用户计算机 108 与输入装置 116 和 118 之间。例如，如同通信路径 P1 所指示的，来自鼠标 116 和键盘 118 的输入数据可通过 USB 连接而被连接到切换系统 102。类似地，如同通信路径 P2 所指示的，切换系统 102 与用户计算机 108 之间的连接同样可以通过 USB 连接发生。如果加密设备 106 是附接于切换设备 104 上的可拆卸设备，那么它可以结合若干个连接器以建立连接性。一旦被附接上，加密设备 106 就通过通信路径 P3 在切换设备 104 之间交换数据。

[0076] 在步骤 204 处，一旦切换系统 102 连接在输入装置 116 和 118 与用户计算机 108（步骤 202）之间，用户就可以启动用户计算机 108 上的应用程序以便在用户计算机 108 的用户与被访问计算机 110 之间提供安全数据通信。一旦启动了应用程序（步骤 204），在步骤 206，该应用程序就与切换设备 104 和加密设备 106 进行通信以便发起如下所进一步描述的鉴别处理。在鉴别用户时，鉴别处理经由切换系统 102 在用户计算机 108 与被访问计算机 110 之间开始安全已加密数据通信会话。

[0077] 在步骤 206，用户计算机 108 上运行的应用程序确定切换系统 102 是否被连接到用户计算机 108。如果切换系统 102 被连接到用户计算机 108 上，则在步骤 208 应用程序提示用户（例如，在显示设备 114 上）使用切换系统 102 来执行鉴别处理。切换系统 102 包括用于提示用户发起鉴别处理的显示设备。例如，除了应用程序（用户计算机 108 上）经由显示设备 114 提示用户之外，切换系统 102 可以结合一个显示设备，提示用户将食指放在与切换系统 102 进行通信或者并入到切换系统 102 之内的指纹检测板上。然后切换系统基于所扫描的指纹来确定用户是否是授权用户。鉴别处理在步骤 209a、209b 和 209c 中举例说明。一旦检测到指纹（步骤 209a），就在步骤 209b 中将它与所存储的参考指纹进行比较，所述参考指纹与切换系统 102 的指定用户（例如，授权使用该设备的用户）有关。如果扫描的指纹和参考指纹相匹配，则切换系统 102 鉴别用户（步骤 209c）。如果在步骤 210 确定了该用户已经被成功地鉴别（例如指纹检测），则在步骤 212，切换系统 102 与用户计算机 108 上运行的应用程序进行通信并且通知该应用程序已经鉴别了该用户。如果在步骤 210 确定了该用户没有被鉴别，如同步骤 208 和 209 所示，用户计算机 108 上运行的应用程序将继续提示该用户使用切换系统 102 继续进行鉴别处理。

[0078] 除如上所述的生物统计学装置外或者作为该装置的替代，也可以把其他鉴别装置引入到切换系统 102 中。例如，在切换系统 102 内，可以使用密码保护和 / 或个人识别码 (PIN) 代码项功能。

[0079] 一旦用户计算机 108 上运行的应用程序收到由切换系统 102 做出的关于已经鉴别

了用户的确认，则在步骤 214 应用程序向切换系统 102 传送安全数据传送的请求。

[0080] 切换系统 102 收到了请求后，如图 4B 所示在步骤 216 中，在切换系统 102 处，从鼠标 116 和键盘 118 所接收的输入数据然后经由切换设备 104 及通信路径 P1 和 P3 被路由给加密设备 106 以便进行加密。通过这种方法，当采用安全通信会话时，输入数据被限制成不加密就不能到达用户计算机 108。

[0081] 在步骤 220 中，切换系统 102 经由通用串行总线 (USB) 连接器把已加密数据发送给用户计算机 108 以便馈送给被访问计算机 110。例如，加密设备 106 根据由用户计算机 108 和被访问计算机 110 的网络接口（例如以太网）来识别的网络协议把已加密数据格式化为网络数据包并且将该网络数据包寻址给被访问计算机 110。网络数据包然后由切换设备 104 沿着通信路径 P3 和 P2b 被路由给用户计算机 108。尽管由 USB 建立了引入到切换系统 102 中的切换设备 104 与用户计算机 108 之间的连接，但是也可以利用其他物理连接器以及传输协议以便在切换系统 102 与用户计算机 108 之间耦合数据。

[0082] 在步骤 222 中，用户计算机 108 上的 USB 连接接收网络数据包，以及由于不把该网络数据包寻址给用户计算机 108，所以把网络数据包提供给用户计算机 108 的网络接口以便通过网络 112 传送给它的寻址目的地，例如被访问计算机 110 上运行的应用程序。

[0083] 在步骤 224，将作为网络数据寻址目的的被访问计算机 110 上运行的应用程序接收并处理包含在该数据包中的已加密输入数据。被访问计算机 110 上运行的应用程序与用户计算机 108 上运行的应用程序有关，借此被访问计算机 110 上运行的应用程序对从切换系统 102 所接收的已加密输入数据进行处理，用户计算机 108 上运行的应用程序从被访问计算机 110 中接收这个已处理数据并且对其进行操作（例如，显示它）。

[0084] 一旦被访问计算机 110 收到了加密输入数据，被访问计算机 110 上的应用程序即可解密这个数据。输入数据包括在与远程网站相关的显示网页上选择一个选项的鼠标点击，所述远程网站是由被访问计算机 110 上的应用程序所运行的。该网页可以被本地访问并显示在与用户计算机 108 有关的显示设备 114 上。该输入数据还包括用于输入被访问网页的一个或多个字段的键盘数据。通常，来自外设的任何数据都可以构成输入数据，所述外设可以与网站或者被访问计算机 110 上运行的应用程序进行数据交换。

[0085] 在步骤 226 中，被访问计算机 110 上运行的应用程序处理该已解密输入数据。基于输入数据，该应用程序产生响应数据以便由用户计算机 108 上运行的应用程序来使用。例如，如果已加密输入数据包括在与被访问计算机 110 上运行的网站有关的网页上的具体特征或选项上进行鼠标点击，被访问计算机 110 上的应用程序就通过产生与用户所选的选项有关的网页图形来处理鼠标点击。因而，被访问计算机 110 上的应用程序通过处理输入数据和产生与该输入数据有关的图形来响应该输入数据。这个响应数据（例如图形数据）被加密并且通过网络 112 发送至切换系统 102（经由用户计算机 108 的网络接口），以便最后通过用户计算机 108 上运行的应用程序作显示处理。用户计算机 108 的网络接口收到已加密响应数据，由于将该数据寻址给切换系统 102 而不是用户计算机 108，所以网络接口把数据传递给用户计算机 108 的 USB 端口和切换系统 102，如通信路径 P5、P4 和 P2b 所示。

[0086] 在步骤 228，并入在切换系统 102 之内的切换设备 104 把已加密响应数据路由给加密设备 106。在加密设备 106 处，已加密响应数据被解密并被送回切换设备 104（路径 P3）。切换设备 104 沿着路径 P2 把该已解密响应数据路由给用户计算机 108 的 USB 连接，或者，

其中由用户计算机 108 上运行的应用程序对该已解密响应数据进行处理。然后该应用程序将已解密响应数据显示在显示设备 114 上（通信路径 P6）。

[0087] 图 4A 和 4B 的实施例中所示的各个步骤举例说明了在加密操作模式期间用户计算机 108 收到所产生的输入数据之前对所产生的输入数据进行加密。这是由通信路径 P1、P3、P2a 来示出的。因而，根据图 3、4a 和 4b 所示的实施例，用户计算机 108 不对这个已加密数据进行本地处理。将其通过通信网络发送到远程的安全站点（例如，被访问计算机 110）以便进行处理。在被访问计算机 110 处，如通信路径 P4 和 P5 所示，对该数据进行解密和处理。一旦被处理，就产生响应数据，所述响应数据被加密并经由用户计算机 108 被发送回切换系统 102。只有在由切换系统 102 解密后，响应数据才被发送给用户计算机 108 以便向用户显示。这就保证了从鉴别源发出响应数据，其中用户正在期待着来自该鉴别源的数据。用户计算机 108 仅处理该响应数据，及显示由另一计算机（例如被访问计算机 110）所执行的处理的结果。这就提供了一种安全的双向链路，其中直接响应被安全传送的输入数据而在安全站点执行处理。

[0088] 用户计算机 108 上运行的应用程序可以从被访问计算机 110 中被下载到用户计算机 108 上或者从切换系统 102 内的存储设备储存在用户计算机 108 上并执行。一旦下载，该应用程序就可以例如在用户计算机 108 上本地执行鉴别程序。换句话说，例如，由应用程序所执行的鉴别程序可以从被访问计算机 110 中进行访问，而不是从用户计算机 108 进行本地访问。根据另一实施例，用户计算机 108 上运行的应用程序可完全从加密设备 106 中被访问和运行。

[0089] 图 5 到 8 是显示根据本发明的实施例在用户计算机 108 上运行的不同应用程序的效果的流程图，所述应用程序在安全操作模式下被激活。在图 3 所示实施例的辅助下来描述这些效果。在系统 100 的安全操作模式期间，用户计算机 108 上运行的应用程序在把已加密输入数据通过网络 112 传送至被访问计算机 110 之前开始鉴别处理。继鉴别之后，用户计算机 108 上运行的安全模式应用程序就成为显示设备 114 上的激活应用程序（例如，如与由激活窗口所表示的应用程序有关的窗口所示那样）。其后，基于用户计算机 108 的用户是否已经决定利用用户计算机 108 上运行的不同应用程序来进行工作，来使与该应用程序有关的窗口被聚焦或者不被聚焦（例如，显示为激活窗口）。图 5 是显示其中当用户计算机 108 上运行的安全模式应用程序不再是激活的应用程序时对本发明的数据通信系统进行操作的方法的流程图。例如，在安全模式应用程序已被激活并且用户已被鉴别之后，用户就可以切换到使用用户计算机 108 上运行的另一应用程序来进行工作。

[0090] 在步骤 300 中，用户计算机 108 上运行的安全模式应用程序接收一个指示，即窗口聚焦已丢失。例如，该安全模式应用程序从用户计算机 108 上的操作系统中接收用于表示应用程序已丢失了窗口聚焦的通知。然后，在步骤 310，用户计算机 108 上运行的安全模式应用程序向切换系统 102 发送表示已退出了安全模式的指示。因此，在步骤 320，切换系统 102 允许输入数据不被加密即可从输入装置 116 和 118 通过通信路径 P2a 流向用户计算机 108。

[0091] 图 6 是显示其中当在用户计算机 108 上恢复安全模式应用程序时对本发明的数据通信系统进行操作的方法的流程图。例如，在安全模式应用程序被激活并且用户已被鉴别之后，用户就可以转而使用用户计算机 108 上运行的另一应用程序来进行工作，这使得安

全模式应用程序丢失了窗口聚焦并且继续运行于后台。此后，用户计算机 108 的用户通过再次选择使用该安全模式应用程序并使其成为激活的应用程序而恢复该安全模式应用程序。

[0092] 在步骤 330 中，用户计算机 108 上运行的安全模式应用程序接收用于表示已经获得了窗口聚焦的指示。例如，安全模式应用程序从用户计算机 108 的操作系统中接收用于表示该应用程序已获得了窗口聚焦的通知。然后，在步骤 340，用户计算机 108 上运行的安全模式应用程序向切换系统 102 发送用于表示已经进入了安全模式的指示。因此，在步骤 380，切换系统 102 把输入数据从输入装置 116 和 118 路由到加密设备 106 以便加密，然后把已加密输入数据经由通信路径 P2b 向上发送至用户计算机 108 以便通过通信路径 P4 和 P4 以及网络 112 传送到被访问计算机 110。

[0093] 图 7 的流程图显示了其中当在用户计算机 108 上恢复安全模式应用程序时对本发明的数据通信系统进行操作的另一种方法。与图 6 的步骤具有相同的参考标号的图 7 的步骤以与图 6 中如上所述的相同方式而被执行。在图 7 中，在安全模式应用程序收到用于表示它已经获得了窗口聚焦的指示（步骤 330）并且通知切换系统 102 已经进入了安全模式（步骤 340）之后，处理继续到步骤 360，其中，在进入安全模式之前，切换系统 102 尝试再次鉴别该用户，例如，采用与结合图 4A 的步骤 209a、209b 和 209c 所在前描述的相同方式。在步骤 370，切换系统 102 判断是否已经鉴别了用户。如果判断为否，则处理回到步骤 360，其中要求用户再次鉴别他自己 / 她自己。如果判断为是，那么处理继续到步骤 380，如以上结合图 6 所描述的那样。

[0094] 图 8 的流程图例示了其中当在用户计算机 108 上恢复安全模式应用程序时对本发明的数据通信系统进行操作的另一种方法。具有与图 6 和 7 的步骤相同的参考标号的图 8 的步骤采用与以上结合这些附图所描述的相同方式来执行。在图 8 中，在安全模式应用程序收到用于表示它已经获得了窗口聚焦的指示（步骤 330）并且通知切换系统 102 已经进入了安全模式（步骤 340）之后，处理继续到步骤 350，其中，在进入安全模式之前，切换系统 102 判断是否已经过去了预定的时间间隔。这个时间间隔可以在生产时被设定或者可由用户来配置。如果判断为否，那么处理继续到步骤 380。如果判断为是，那么如以上结合图 7 的步骤 360 和 370 所描述的那样，切换系统 102 在进入安全模式之前尝试再次对用户进行鉴别。

[0095] 图 9 是举例说明根据本发明的实施例的切换系统的组件的框图。切换系统 400 包括处理器 402（例如，由 Freescale Semiconductor, Inc. 提供的 MC9328MXL）、存储设备 404（例如 PSRAM 和闪速存储器）、显示器 406（例如，彩色 OLED 显示器）、指纹扫描仪 408（例如，由 Atmel 提供的 FingerChip ® AT77C104B）、音频编码器 / 解码器 410（例如，由 VLSI SolutionOy 提供的 VS1002D）、外部连接器 412 以及 USB 控制器设备 414（例如，由 Cypress Semiconductor Corp. 提供的 CYC67200）。如以下所进一步讨论的那样，处理器 402 基于存储在存储设备 404 上的程序来执行如上所述的切换系统的功能（例如，切换、加密以及解密）。如以下所进一步讨论的那样，处理器 402 还与切换系统 400 的其他组件的行动相协作。同样存储在存储设备 404 上的控制程序（称为切换系统控制程序或者 SSCP）控制处理器 402 的行动，如以下所进一步讨论的那样。

[0096] 处理器 402 包括 USB 设备模块组合，所述 USB 设备模块组合用于使处理器 402 起

到能实现多种不同功能的USB设备的作用。每个这种功能都属于标准USB设备类。例如，如以下所进一步描述的那样，一旦处理器402连接到USB主机上，USB设备模块就使处理器402能够被识别为（例如，被USB主机）并且被用作USB大容量存储器和USB通信设备（例如，以太网仿真设备）。

[0097] 显示器406向切换系统的用户提供显示器以便接收各种提示。例如，显示器406提示用户将他们的食指放在指纹扫描仪408上（例如，“将食指放在扫描板上”）。显示器406还可以向用户提供与他和用户计算机之间的连接的建立有关的状态信息（例如“检测到连接失败”）。

[0098] 存储设备404为切换系统400提供了存储器。如上所述，存储设备404存储由处理器402执行的程序。存储设备404还存储扫描到的指纹数据、各种加密/解密程序数据、数据缓存、控制程序数据及其他数据。

[0099] 指纹扫描仪408包括指纹检测板和用于产生与用户指纹有关的数据（例如，如存储在存储设备404中那样）的扫描仪。在鉴别期间，将扫描的指纹与用户指纹的鉴别副本相比较。当鉴别副本与用户指纹的扫描副本相同或相关联时，认为完成了鉴别。

[0100] 音频编码器/解码器410向用户提供多个音频相关选项。例如，从外部连接器412所接收到的声音数据可以由设备410进行数字化并且编码为声音数据文件。声音数据被存储在存储器404中并在通信网络上被传送至另一计算机。继在设备410中的编码处理之后还将其直接传送给远程位置。还利用编码器/解码器410来处理所存储的（例如存储器404）或所下载的声音文件（例如，MP3音乐文件）以便进行播放。

[0101] 外部连接器412包括USB插槽、麦克风输入插座和/或音频输出端（例如，耳机插槽）。例如，把存储器404中所存储的已解码音频音乐文件输出到耳机插座。

[0102] USB控制器设备414用作USB集线器将处理器402和一个或多个输入产生设备（例如鼠标和键盘）连接到用户计算机108（图1）。图10显示了控制器设备414的详细情况。

[0103] 控制器设备414包括具有相应串行接口引擎(SIE)431的第一USB端口430、具有相应SIE 433的第二USB端口432、通用I/O(GPIO)接口436以及处理器438。USB端口430在控制器414和用户计算机108之间提供连接性。同样地，USB端口432将输入装置116和118（例如鼠标和键盘）连接至控制器设备414。处理器402通过GPIO接口436与控制器设备414通信。处理器402通过GPIO接口436向控制器414发送和从控制器414接收数据（例如输入数据、控制数据和应用数据）。

[0104] 通过回头参考上述图4A到6，并且在切换系统400的环境中详细描述其流程图来进一步描述切换系统400。参考图4A，在步骤202，切换系统连接到用户计算机和输入设备。一旦连接，用户计算机108（在该实施例中包括USB主机系统）将切换系统400识别为USB集线器，组合USB设备（如上所述，包括USB大容量存储器功能和USB以太网仿真设备功能）附接于USB集线器上。用户计算机108同样将输入设备116和118识别为附接于集线器的USB输入设备。一旦连接了切换系统400，就在处理器402处初始化切换系统控制程序(SSCP)。

[0105] 此外，一旦连接了切换系统400，就建立了多个逻辑通信信道，例如对应于每个USB设备的一条或多条USB管线。在切换系统400的环境中，如上所述的逻辑通信路径P2a和P2b分别对应于与人机界面设备(HID)类设备（例如，输入装置116和118）有关的全部

信道以及对应于与以太网仿真设备功能有关的信道。

[0106] 在首次连接时，切换系统 400 在非安全模式下运行。在这种模式下，USB 控制器的处理器 438 命令 SIE 433 将其从 I/O 端口 432 所接收的数据（例如，从连接到 I/O 端口 432 的输入装置 116 和 118 中所接收的输入数据）发送至 SIE 431，SIE 431 把该数据经由 I/O 端口 430 发送给用户计算机 108 的 USB 主机系统。

[0107] 在步骤 204，用户计算机 108 上执行的安全模式应用程序被启动。如上所述，可将这个应用程序存储在切换系统 400 的存储设备 404 中。同样地，把应用程序提交（例如，由用户计算机 108 的操作系统的文件系统）给用户作为存储在 USB 大容量存储设备中的可执行文件。然后用户计算机 108 处的用户采用与用户计算机 108 的操作系统有关的传统方式启动应用程序（例如，双击代表与该应用程序相对应的文件的图标）。

[0108] 在步骤 206，用户计算机上运行的安全模式应用程序判断是否连接了切换系统。这是由安全模式应用程序经由集成在切换设备 104（图 3）中的 USB 控制器来提出关于切换系统 102（图 3）的提交的询问而实现的。在与切换系统 102（图 3）有关的连接和鉴别处理期间，应用程序与远程系统 110（图 3）进行通信。

[0109] 在用户计算机上运行的安全模式应用程序提示用户使用切换系统来鉴别他们自己（步骤 208）之后，切换系统尝试根据步骤 209a、209b 以及 209c 来鉴别用户。这是由切换系统控制程序来实现的，所述切换系统控制程序启动存储于存储设备 404 的鉴别程序以便使处理器 402 按照前述方式来执行步骤 209a、209b 以及 209c，其中处理器 402 利用显示器 406 来提示用户并且利用指纹扫描仪 408 获得来自用户的指纹数据。

[0110] 在步骤 212，切换系统通知用户计算机上运行的安全模式应用程序已经鉴别了用户。这是通过切换系统控制程序向用户计算机 108 上运行的安全模式应用程序发送指示来实现的。

[0111] 在步骤 214，用户计算机上运行的安全模式应用程序请求开始安全模式。这是通过用户计算机 108 上运行的安全模式应用程序经 USB（即链路 P2）向切换系统控制程序发送指示来实现的。

[0112] 当收到启动安全模式的这个请求时，切换系统控制程序经由 GPIO 接口 436 向 USB 控制器处理器 438 发送一个指令，命令它进入安全模式。然后 USB 控制器处理器 438 命令 SIE 433 停止向 SIE 431 路由数据，改为经由 GPIO 接口 436 把数据从 USB 端口 432 路由给处理器 402。无需改变连接于 I/O 端口 432 的输入设备的 USB 状态即可改变这一路由。因此，对于用户计算机上的 USB 主机系统而言，尽管在安全模式期间来自 USB 输入设备的数据被阻止上行流入 USB 主机系统中，但是 USB 输入设备（例如鼠标 116 和键盘 118）仿佛仍然被连接并且完全可操作。

[0113] 如果期望，则可以对 USB 控制器处理器 438 进行配置，以便只要通过特定的通信路径（例如 GPIO 接口 436）收到命令就会识别出该命令从而进入安全模式。其优点在于提高了从处理器 402 而不是从驻留于用户计算机上的流氓程序中接收进入安全模式的命令的可能性。

[0114] 现在参考图 4B，在步骤 216，切换系统收到输入数据并且该输入数据被发送至加密设备以便加密。在切换系统 400 环境下，在安全模式期间，SIE 433 经由 I/O 端口 432 接收来自输入设备 116 和 118 的数据并且将其通过 GPIO 436 路由给处理器 402。然后，处理

器 402 上运行的切换系统控制程序执行来自存储设备 404 的加密程序以便加密该数据。

[0115] 在步骤 220，切换系统将已加密数据格式化为网络数据包并且将其发送给用户计算机。在切换系统 400（图 9）的环境下，切换系统控制程序接收来自加密程序的已加密数据并且命令 USB 以太网仿真设备类功能把该已加密数据发送到被访问计算机 110 的 IP 地址。由远程被访问系统 110（图 3）的动态主机控制协议（DHCP）分配作为已加密数据发送目的地的 IP 地址。USB 以太网仿真设备类功能根据以太网协议来格式化已加密数据并且把这个以太网数据包封装为 USB 数据并且通过以太网数据包（包含已加密输入数据）把这个 USB 数据发送给用户计算机 108 的 USB 主机系统。

[0116] 在步骤 222，将网络数据包发送给被访问计算机上运行的安全模式应用程序。在包括切换系统 400 的本实施例的环境下，用户计算机 108 的 USB 主机系统在收到该以太网数据包时将其传送至用户计算机 108 的网络接口以便通过网络 112 传送给被访问计算机 110。

[0117] 在被访问计算机 110 收到以太网数据包（步骤 224）之后，它解密并处理其中所包含的已加密输入数据以产生响应，加密该响应，并且把该已加密响应传送给切换系统（步骤 226）。

[0118] 在步骤 228，切换系统接收并解密该已加密响应，并且把已加密响应发送给用户计算机上运行的应用程序以便操作。在包括切换系统 400 的本发明实施例的环境下，包含来自被访问计算机 110 的已加密响应的以太网数据包到达用户计算机 108 的网络接口。由于这个以太网数据包被寻址给切换系统 400 的 USB 以太网仿真设备类功能，所以把以太网数据包传递给用户计算机 108 的 USB 主机系统，其把以太网数据包打包到 USB 包中，以便通过该 USB 进行传送。在 SIE 431 处接收这个 USB 包，并把这个 USB 包经由 GPIO 接口 436 路由给处理器 402 上运行的 USB 以太网仿真设备类功能。在处理器 402，USB 以太网仿真设备类功能从该以太网数据包中提取已加密响应数据，并将其传递给切换系统控制程序，所述切换系统控制程序从存储设备 404 中启动解密程序以便解密该响应。然后，切换系统控制程序把这个已解密响应数据发送给用户计算机 108 上运行的安全模式应用程序。切换系统控制程序与用户计算机 108 上运行的安全模式应用程序之间的通信通过 USB 来进行。用户计算机 108 上运行的安全模式应用程序将切换系统看作为 USB 以太网设备并且通过 USB 接口经由以太网与其进行通信。

[0119] 如上所述，图 5 和 6 描述了用户计算机 108 上运行的不同应用程序的效果，在根据本发明实施例的安全运行方式条件下变为激活的程序的效果。如前所述，图 5 是显示其中当用户计算机 108 上运行的安全模式应用程序不再是激活的应用程序时对本发明的数据通信系统进行操作的方法的流程图。参考图 5，用户计算机 108 上运行的安全模式应用程序收到了用于表示已经失去了窗口聚焦的指示（步骤 300）。然后，在步骤 310，用户计算机 108 上运行的安全模式应用程序向切换系统 102 发送用于表示已经退出了安全模式的指示。在包括切换系统 102 的本发明实施例的环境下，这可以通过安全模式应用程序向切换系统控制程序发送用于表示已经退出了安全模式的指示来实现。这是经由 USB 的终点通信信道来获得的，其中由用户计算机 108 的 USB 驱动接口（即 USB 主机设备）将切换系统 102（即终点设备）标识成以太网设备。

[0120] 在步骤 320，切换系统把输入数据不经加密就从输入设备通过通信路径 P2a 流向用户计算机。在切换系统 400 的环境下，经由 GPIO 接口 436 向 USB 控制器处理器 438 发送

指令，命令它进入非安全模式。然后 USB 控制器处理器 438 命令 SIE 433 将它从 I/O 端口 432 接收到的数据路由到 SIE431，所述 SIE 431 经由 I/O 端口 430 把这一数据发送给用户计算机 108 上的 USB 主机系统。

[0121] 如前所述，图 6 是显示其中当在用户计算机 108 上恢复安全模式应用程序时对本发明的数据通信系统进行操作的方法的流程图。参考图 6，在运行于用户计算机 108 上的安全模式应用程序收到用于表示已经获得了窗口聚焦的指示（步骤 330）之后，它向切换系统发送用于表示已经进入了安全模式的指示（步骤 340）。在包括切换系统 400 的本发明实施例的环境下，后一步骤可以通过安全模式应用程序向切换系统控制程序发送用于表示已经进入了安全模式的指示来实现。

[0122] 然后，在步骤 380，切换系统将数据从输入设备路由到加密设备 106 以便进行加密，然后经由通信路径 P2b 把已加密输入数据上行发送到用户计算机以便传送给被访问计算机。在切换系统 400 的环境下，这可以通过切换系统控制程序经由 GPIO 接口 436 向 USB 控制器处理器 438 发送指令，命令它进入安全模式来实现。然后，USB 控制器处理器 438 命令 SIE 433 停止向 SIE 431 路由数据，改为经由 GPIO 接口 436 把数据从 USB 端口 432 路由给处理器 402。然后来自输入设备 116 和 118 的输入数据被路由给切换系统控制程序以便加密，并且以如上所述的相同方式被发送给被访问计算机 110。

[0123] 图 11A 和 11B 举例说明了引入了切换系统 102（图 3）的系统的替换实施例。在图 11A 中，一般被引入到计算机（例如，图 3 所示的计算机 108）中的网络接口 502 可以被集成到切换系统 504 中。在该实施例中，直接通过网络 506 把已加密数据发送给服务器或者远程计算机 508 以便处理。如果设备 504 被用于访问不要求加密 / 解密和 / 或鉴别的另一个网站，则它将在非安全模式下运作。在非安全模式下，切换设备 512 把由接口 502 从另一个网站所接收的数据路由给加密设备 505。在加密设备 505 处，由加密设备对所接收的数据进行处理（不是加密 / 解密），并且经由切换设备 512 将其发送给显示设备 510。例如，加密设备 505 包括用于提供因特网访问的因特网浏览器程序。将所访问的网页数据从远程服务器（例如，计算机 508）通过通信网络 506 发送到切换系统 504，其中由接口 502 来接收该数据。从接口 502 中，切换设备 512 把所接收的网页数据路由给加密设备 505。然后，在由切换设备 512 路由给显示设备 510 之前，由运行于加密设备 505 上的浏览器程序对该网页数据进行处理。

[0124] 然而，如果在安全模式下使用设备 504，一旦加密设备 505 对从远程计算机 508 中所接收的加密数据进行解密，就将所接收的已解密数据显示在显示设备 510 上。显示设备 510 包括显示驱动器（例如，VGA 卡）和连接于安全设备 504 的监视器。在图 11B，除了设备 516（图 11B）包括集成显示设备以外，安全设备 516 与安全设备 504（图 11A）相同。集成显示设备可以被并入到加密设备 518 内（参见图 4，显示器 406）。换句话说，专用显示设备可以被直接附接到该安全设备 516 上。图 11A 和 11B 中举例说明的安全设备 504 和 516 分别包括多个显示驱动器以便利用不同的外部显示设备来进行使用。因此，每个设备 504、516 可以合并有用于支持与这些显示设备的连接的一个或多个外部连接器。

[0125] 在结合优选实施例来描述和例示本发明时，在不脱离本发明的精神和范围之下，可以做出对所属领域技术人员来说显而易见的许多改变和改进，因此，由于这种改变和改进应当被包括在本发明的范畴内，所以本发明不应被限制在上述方法或结构的具体细节之

内。除了程序上需要或者固有于处理本身之中之外，本说明书（包括附图）中所描述的方法或者处理的步骤或者阶段的具体顺序不是固有的。多数情况下，无需改变所描述的方法的目的、效果或含义就可以改变处理步骤的顺序。

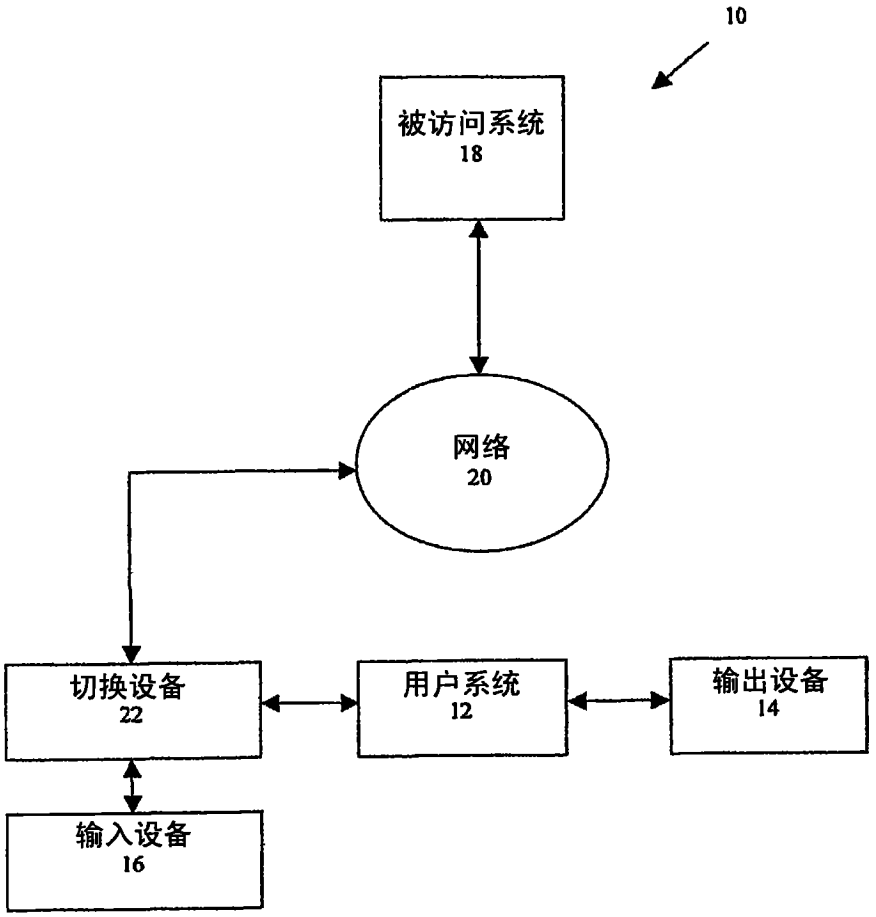


图 1

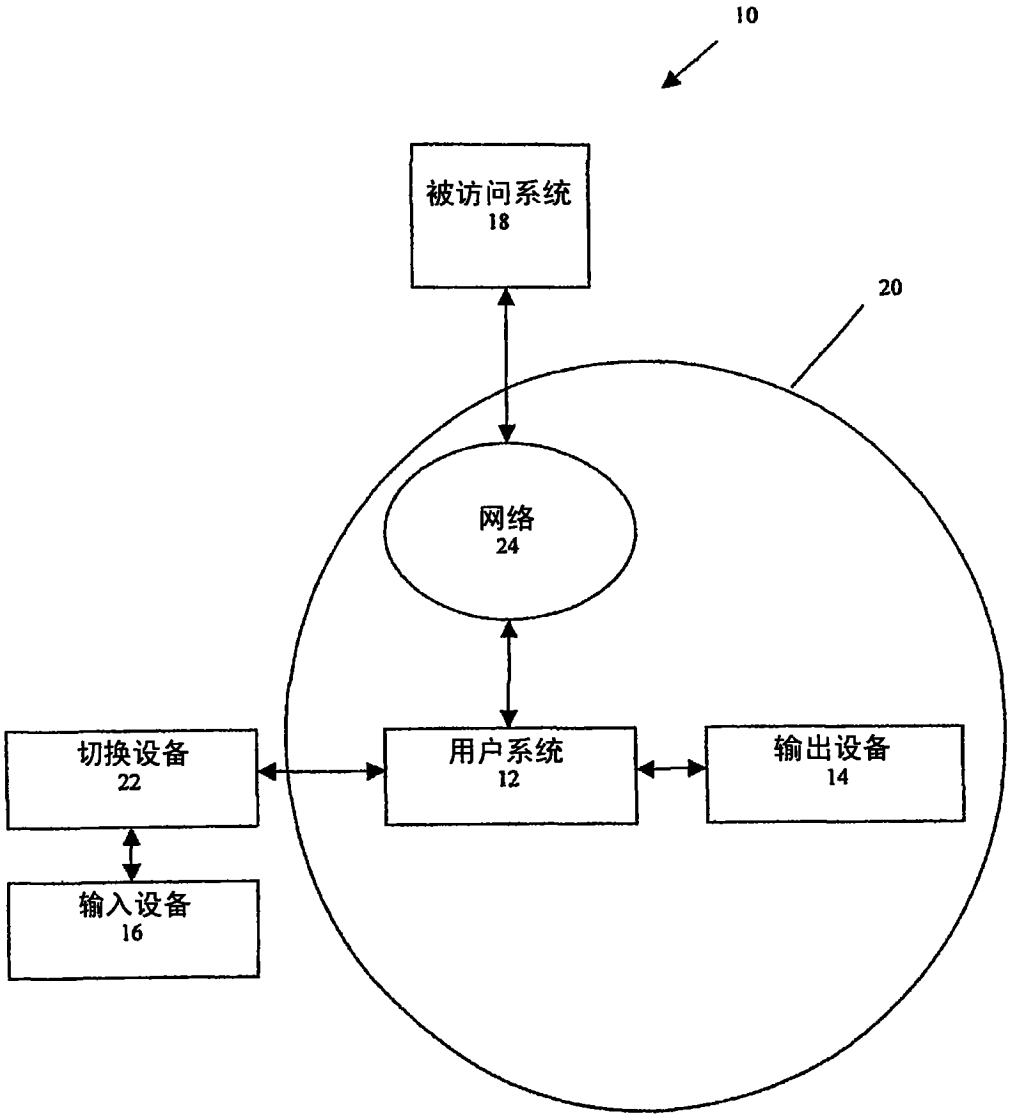


图 2

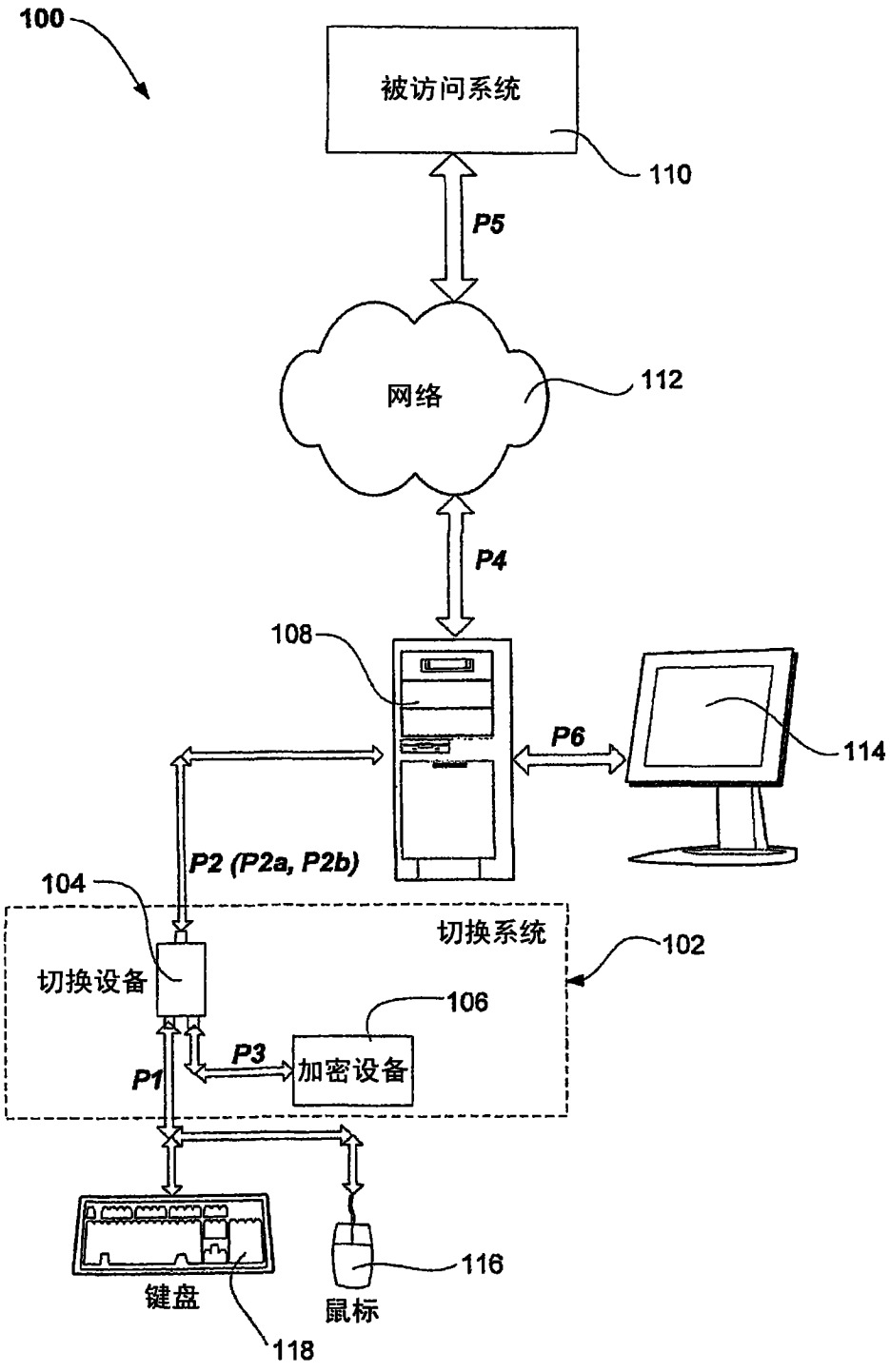

100
被访问系统
110
P5
网络
112
P4
108
P6
114
P2 (P2a, P2b)
104
切换系统
102
切换设备
106
P3
P1
加密设备
116
键盘
鼠标
118

图 3

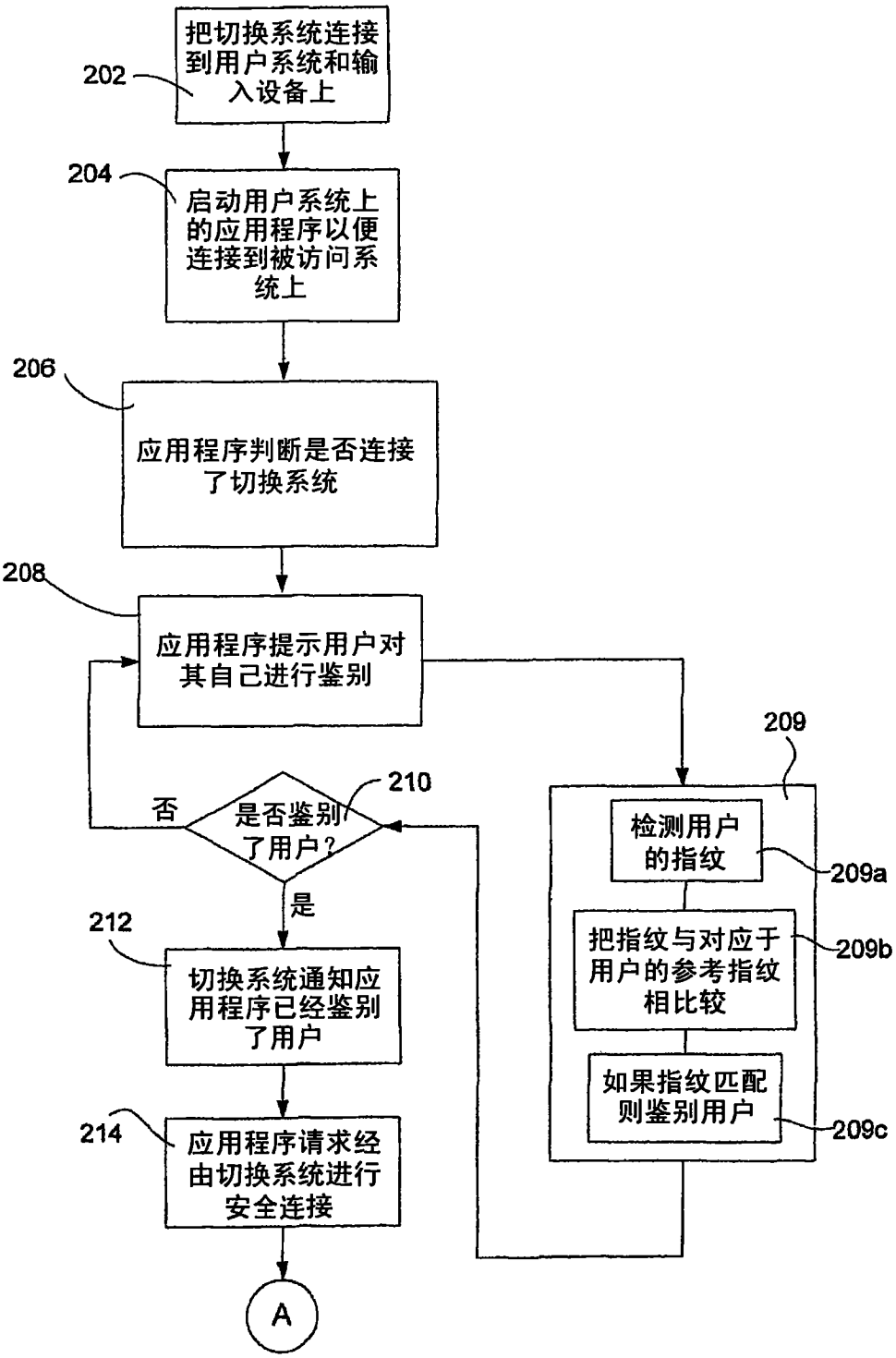

把切换系统连接到用户系统和输入设备上
202
启动用户系统上的应用程序以便连接到被访问系统上
204
应用程序判断是否连接了切换系统
206
应用程序提示用户对其自己进行鉴别
208
209
检测用户的指纹
209a
把指纹与对应于用户的参考指纹相比较
209b
如果指纹匹配则鉴别用户
209c
是否鉴别了用户？
210
否
是
切换系统通知应用程序已经鉴别了用户
212
应用程序请求经由切换系统进行安全连接
214
A

图 4A

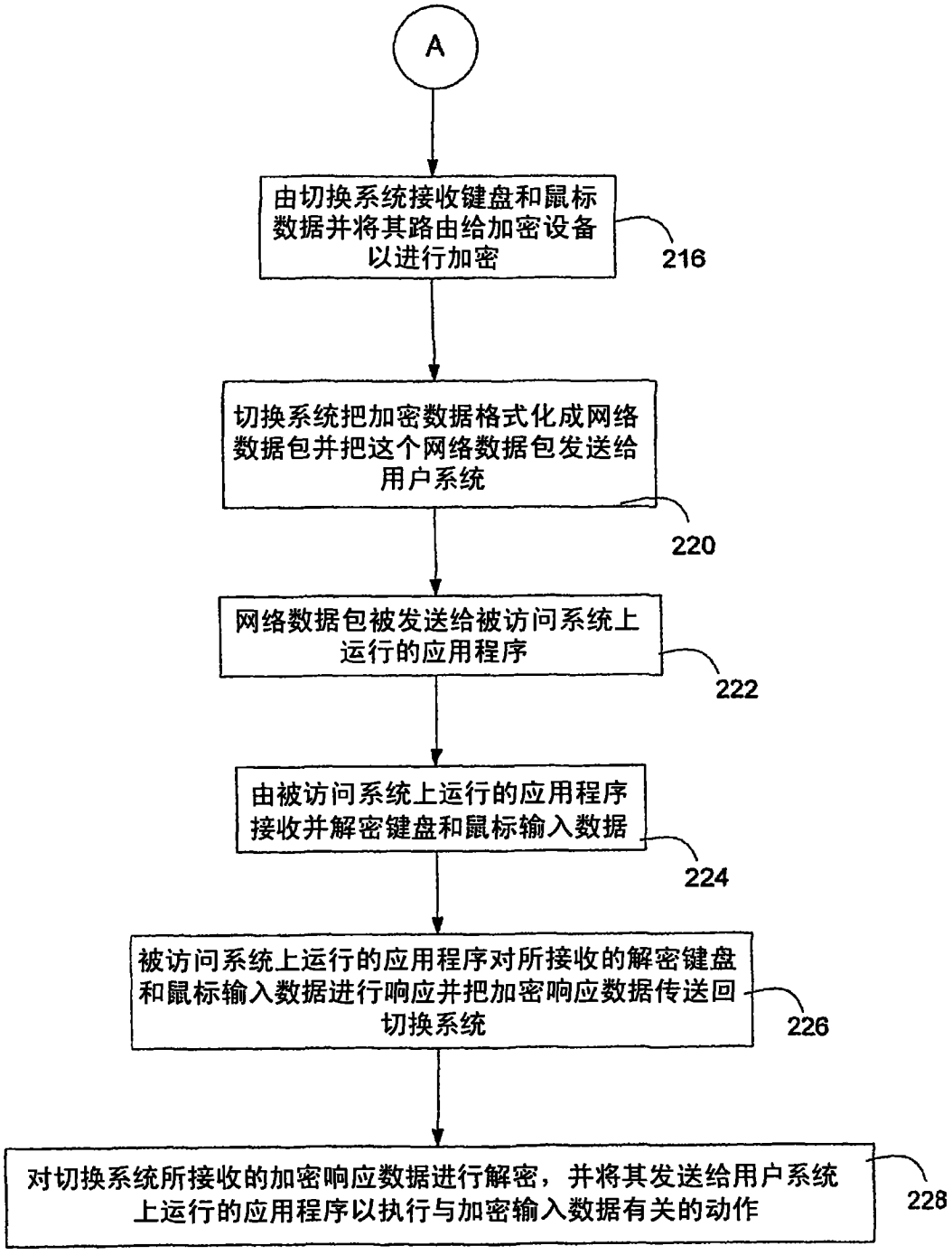

A
由切换系统接收键盘和鼠标数据并将其路由给加密设备以进行加密
216
切换系统把加密数据格式化成网络数据包并把这个网络数据包发送给用户系统
220
网络数据包被发送给被访问系统上运行的应用程序
222
由被访问系统上运行的应用程序接收并解密键盘和鼠标输入数据
224
被访问系统上运行的应用程序对所接收的解密键盘和鼠标输入数据进行响应并把加密响应数据传送回切换系统
226
对切换系统所接收的加密响应数据进行解密，并将其发送给用户系统上运行的应用程序以执行与加密输入数据有关的动作
228

图 4B

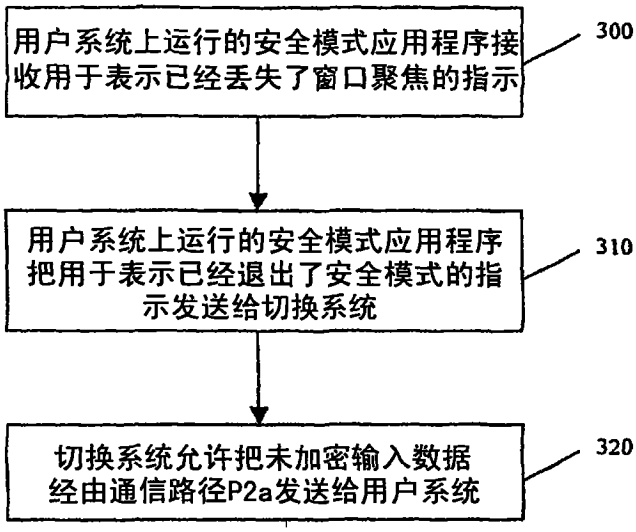

用户系统上运行的安全模式应用程序接收用于表示已经丢失了窗口聚焦的指示
300
用户系统上运行的安全模式应用程序把用于表示已经退出了安全模式的指示发送给切换系统
310
切换系统允许把未加密输入数据经由通信路径P2a发送给用户系统
320

图 5

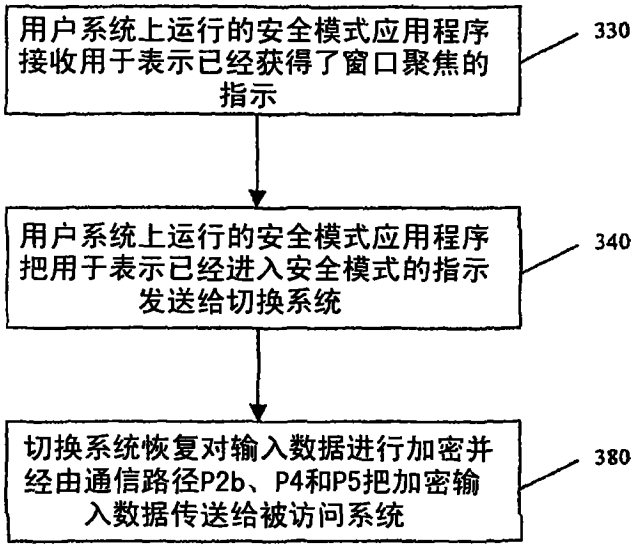

用户系统上运行的安全模式应用程序接收用于表示已经获得了窗口聚焦的指示
330
用户系统上运行的安全模式应用程序把用于表示已经进入安全模式的指示发送给切换系统
340
切换系统恢复对输入数据进行加密并经由通信路径P2b、P4和P5把加密输入数据传送给被访问系统
380

图 6

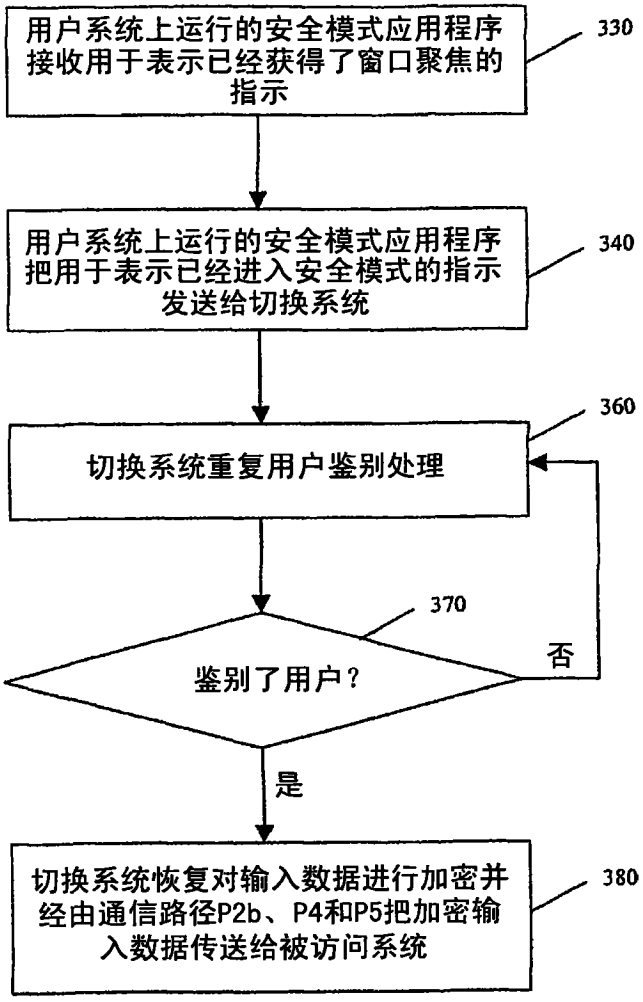

用户系统上运行的安全模式应用程序接收用于表示已经获得了窗口聚焦的指示
330
用户系统上运行的安全模式应用程序把用于表示已经进入安全模式的指示发送给切换系统
340
切换系统重复用户鉴别处理
360
鉴别了用户？
370
否
是
切换系统恢复对输入数据进行加密并经由通信路径P2b、P4和P5把加密输入数据传送给被访问系统
380

图 7

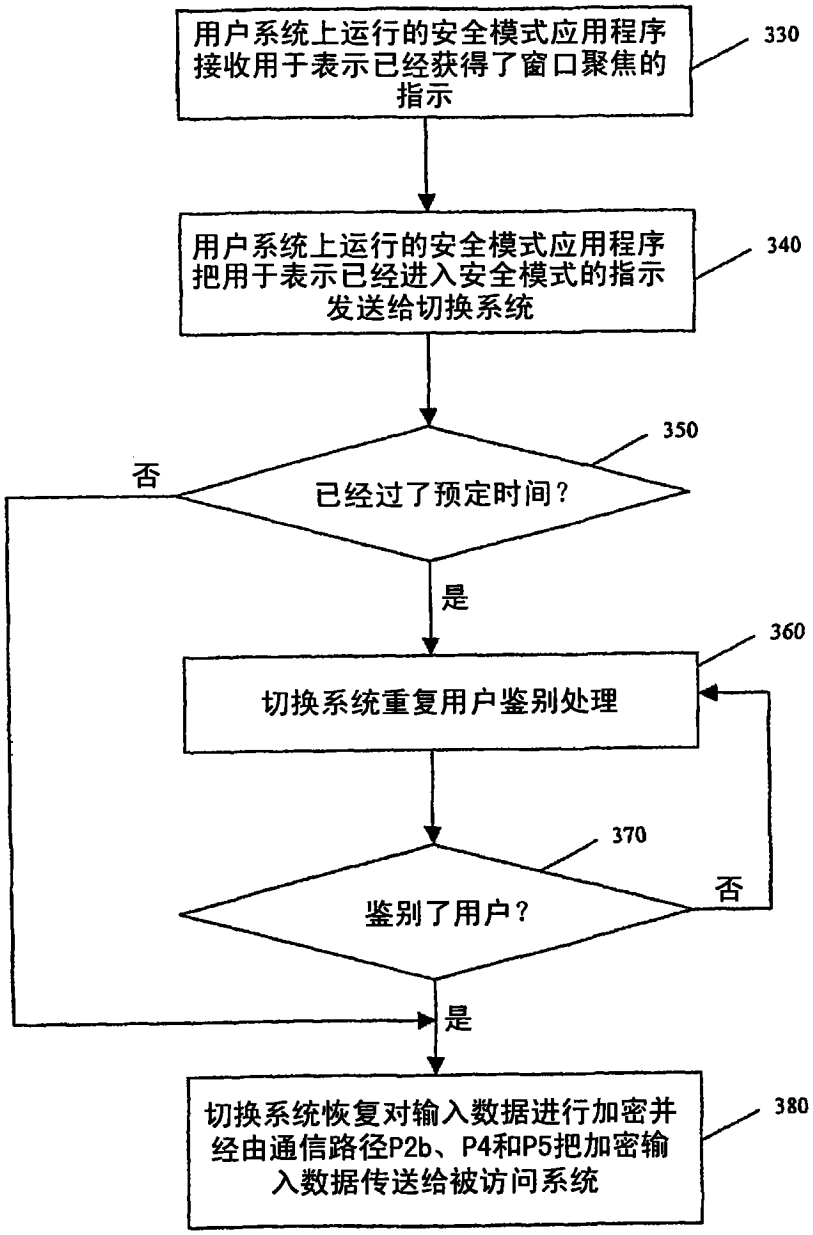

用户系统上运行的安全模式应用程序接收用于表示已经获得了窗口聚焦的指示
330
用户系统上运行的安全模式应用程序把用于表示已经进入安全模式的指示发送给切换系统
340
350
已经过了预定时间？
否
是
360
切换系统重复用户鉴别处理
370
鉴别了用户？
否
是
切换系统恢复对输入数据进行加密并经由通信路径P2b、P4和P5把加密输入数据传送给被访问系统
380

图 8

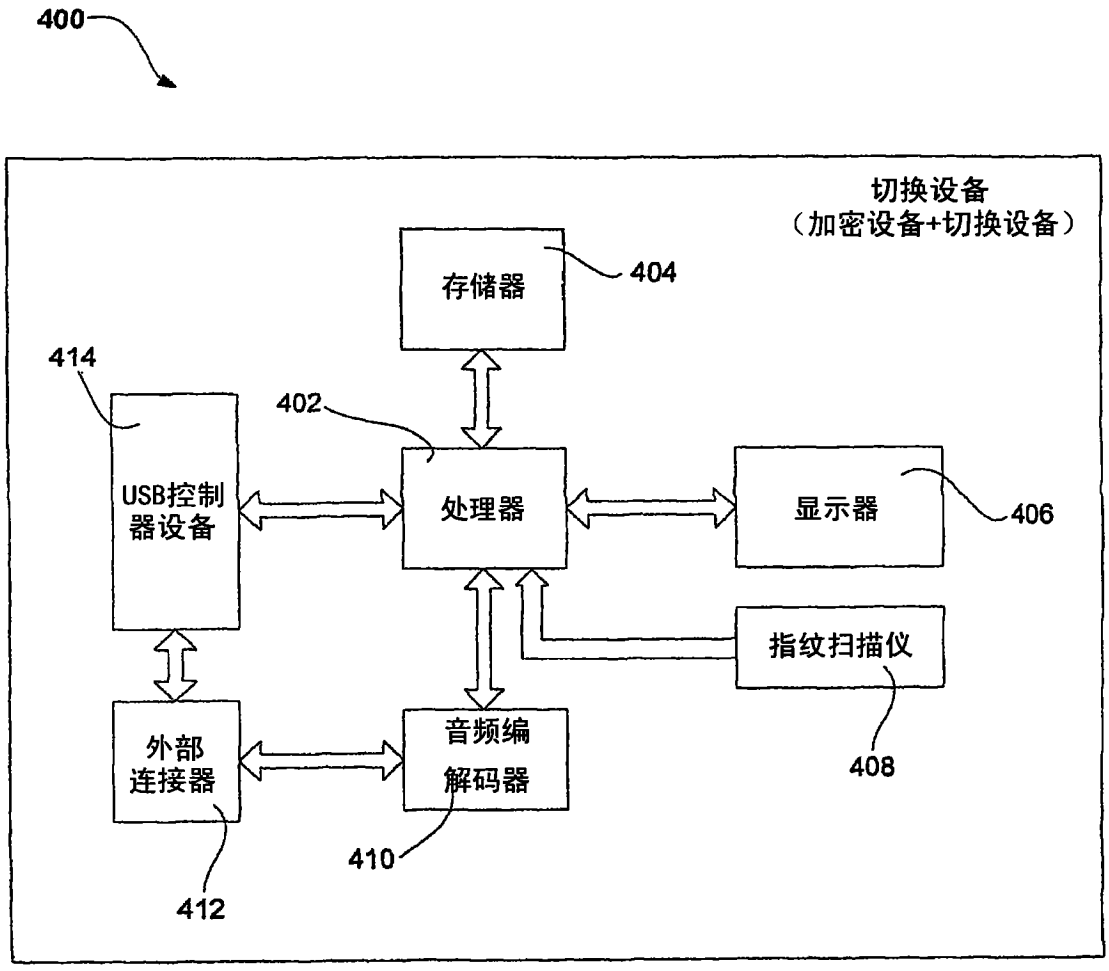

400
切换设备
（加密设备+切换设备）
存储器
404
414
402
USB控制
器设备
处理器
显示器
406
指纹扫描仪
408
外部
连接器
音频编
解码器
410
412

图 9

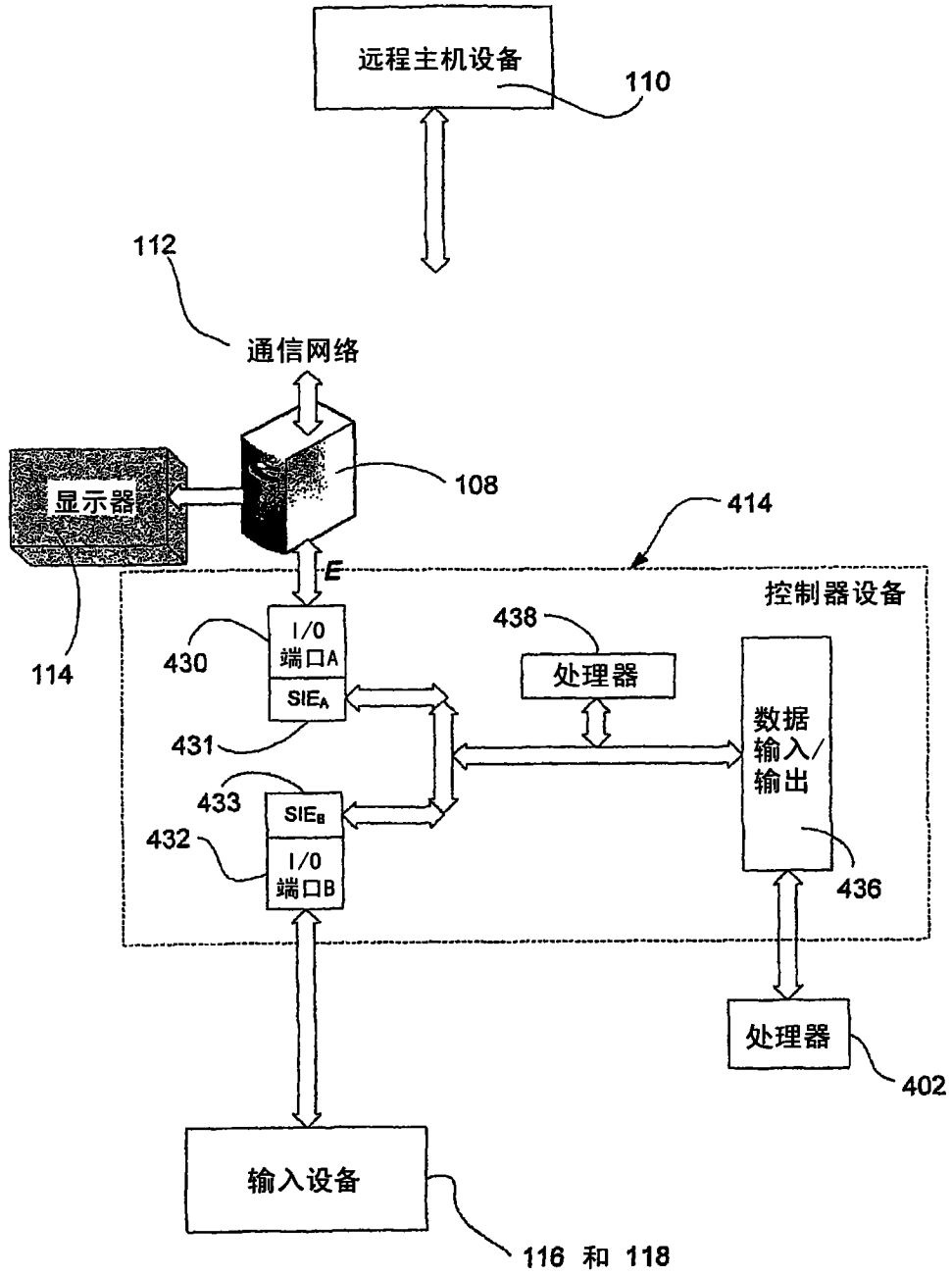

远程主机设备
110
112
通信网络
显示器
108
414
E
控制器设备
I/O
端口A
SIE_A
430
438
处理器
数据
输入/
输出
431
433
SIE_B
432
I/O
端口B
436
处理器
402
114
输入设备
116 和 118

图 10

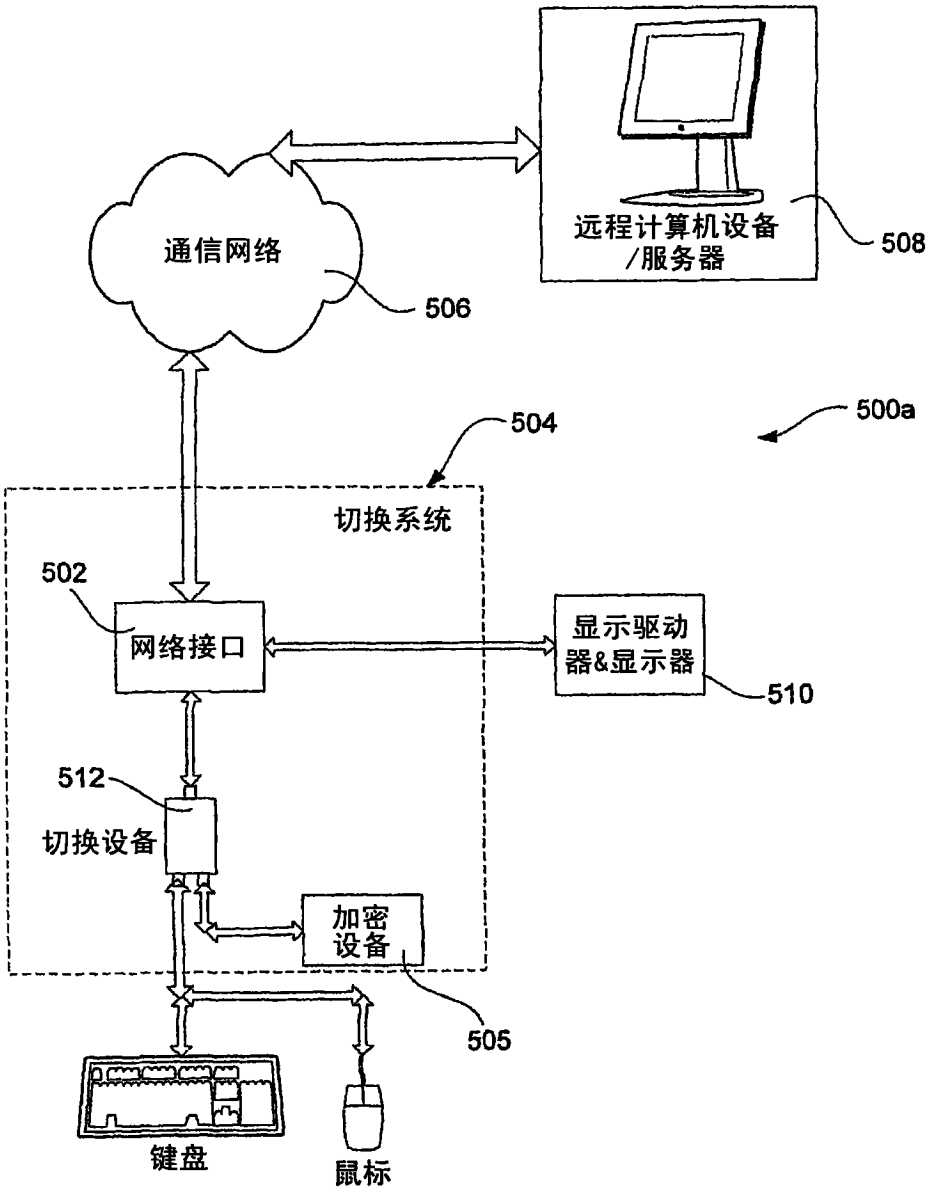

通信网络
506
远程计算机设备
/服务器
508
500a
504
切换系统
502
网络接口
显示驱动
器&显示器
510
512
切换设备
加密
设备
505
键盘
鼠标

图 11A

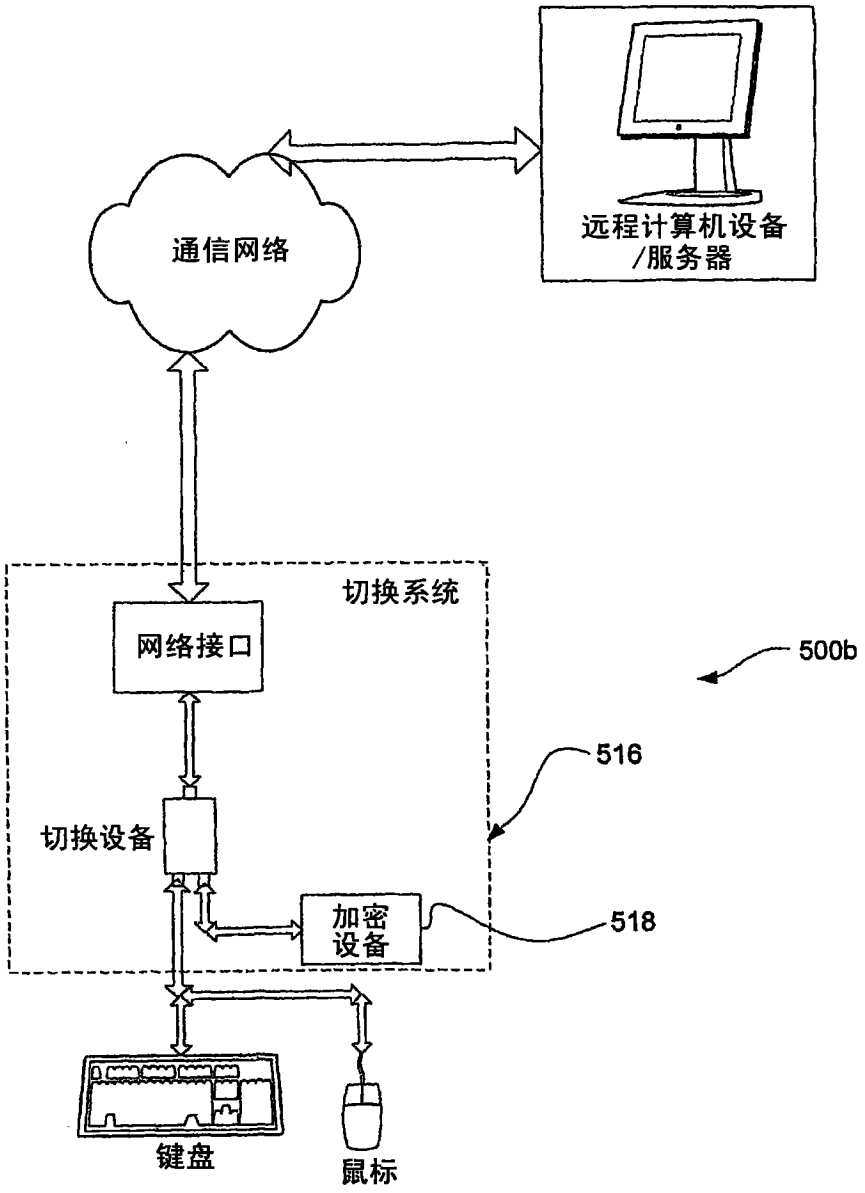


图 11B