Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2650163 C 2013/07/23

(11)(21) 2 650 163

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(22) Date de dépôt/Filing Date: 2008/12/18

(41) Mise à la disp. pub./Open to Public Insp.: 2010/06/18

(45) Date de délivrance/Issue Date: 2013/07/23

(51) Cl.Int./Int.Cl. *H04L 9/32* (2006.01),
G06F 21/31 (2013.01), *G06Q 20/40* (2012.01)

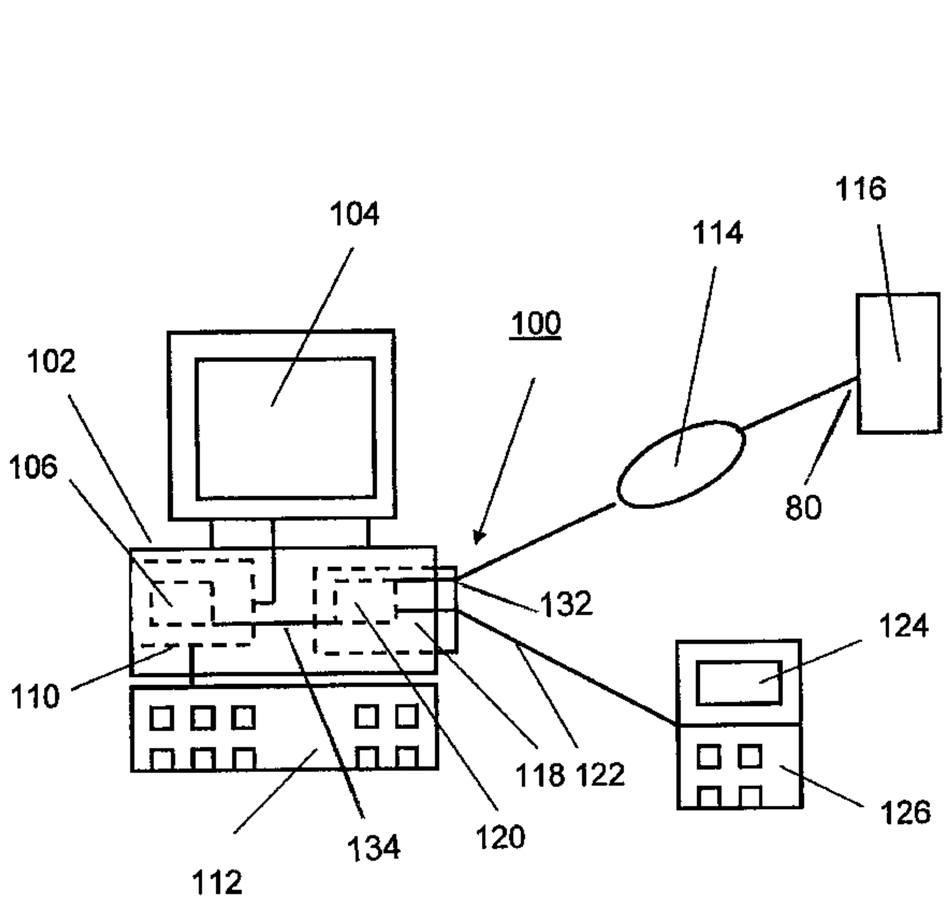
(72) Inventeur/Inventor:
MCALEAR, JAMES A., CA

(73) Propriétaire/Owner:
MCALEAR, JAMES A., CA

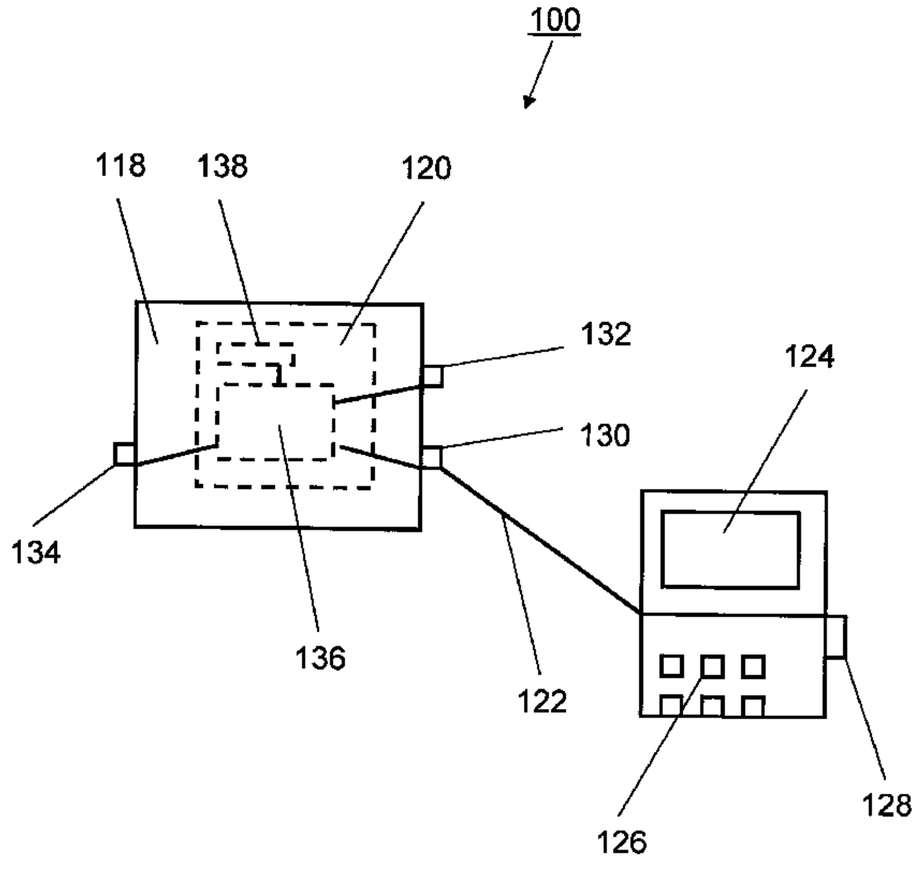
(74) Agent: CASSAN MACLEAN

(54) Titre : SYSTEME ET PROCEDE POUR LA FOURNITURE SECURISEE DE RENSEIGNEMENTS D'IDENTIFICATION CLES

(54) Title: SYSTEM AND METHOD FOR SECURE PROVISION OF KEY CREDENTIAL INFORMATION



A



B

(57) Abrégé/Abstract:
A system for secure provision of key credential information is provided. The system comprises secure logic circuitry for being disposed in a host computer. The secure logic circuitry detects a message received from a remote computer connected to the host computer and indicative of a request for provision of the key credential information; generates a message for prompting a user for provision of the key credential information; receives the key credential information; and provides the key credential information to the remote computer absent processing using circuitry of the host computer. The system further comprises a secure user interface connected to the secure logic circuitry for receiving the key credential information from the user and providing the same to the secure logic circuitry.

ABSTRACT

A system for secure provision of key credential information is provided. The system comprises secure logic circuitry for being disposed in a host computer. The secure logic circuitry detects a message received from a remote computer connected to the host computer and indicative of a request for provision of the key credential information; generates a message for prompting a user for provision of the key credential information; receives the key credential information; and provides the key credential information to the remote computer absent processing using circuitry of the host computer. The system further comprises a secure user interface connected to the secure logic circuitry for receiving the key credential information from the user and providing the same to the secure logic circuitry.

SYSTEM AND METHOD FOR SECURE PROVISION OF KEY CREDENTIAL INFORMATION

FIELD OF THE INVENTION

The present invention relates to computer networking, and more particularly to a system for secure provision of key credential information to a server via an un-trusted computer.

BACKGROUND OF THE INVENTION

Commerce over the Internet has become very popular. Such commerce takes many forms, from purchasing merchandize from online vendors to conducting online banking and stock trading. Common to all such transactions is the need to transmit private secure information. Typically, the transactions are carried out using secure encrypted connections. However, there are still opportunities to capture the private information that is used during online transactions, for example, to obtain passwords, Personal Identification Numbers (PIN), social security numbers, driver's license numbers and account numbers, to name a few. Illegal procurement of such information and using the same in a fraudulent manner is commonly referred to as identity theft.

While the Internet is by far the largest and most pervasive computer network, the problem of identity theft occurs in other networks as well. For example, identity theft can occur entirely within the confines of a corporate network or a university network wherein a dishonest individual uses a transaction within the network to steal PINs enabling access to confidential information.

Many of the current security mechanisms assume that a user's computer and its keyboard are secure, which is incorrect. One form of conducting online identity theft is to use a keystroke logger to log individual keystrokes for extracting personal information. The keystroke logger is, for example, software installed on a computer without the user's knowledge and its operation is invisible to the user. The keystroke logger in the form of software is, for example, distributed and installed remotely – for example, in the form of malware – and transmits the key logs to a remote computer in an invisible fashion. Numerous anti-virus programs fight known malicious

software programs and try to keep up with the proliferation of new malicious software programs.

It is desirable to provide a system for secure provision of key credential information to a server via an un-trusted computer.

It is also desirable to provide a system for secure provision of key credential information that is easily installed in an existing computer system.

SUMMARY OF THE INVENTION

Accordingly, one object of the present invention is to provide a system for secure provision of key credential information to a server via an un-trusted computer.

Another object of the present invention is to provide a system for secure provision of key credential information that is easily installed in an existing computer system.

According to one aspect of the present invention, there is provided a system for secure provision of key credential information. The system comprises secure logic circuitry for being disposed in a host computer. The secure logic circuitry detects a message received from a remote computer connected to the host computer which is indicative of a request for provision of the key credential information; generates a message for prompting a user for provision of the key credential information; receives the key credential information; and provides the key credential information to the remote computer absent processing using circuitry of the host computer. The system further comprises a secure user interface connected to the secure logic circuitry for receiving the key credential information from the user and providing the same to the secure logic circuitry.

According to another aspect of the present invention, there is further provided a method for secure provision of key credential information. Using a secure logic circuitry disposed in a host computer, a message received from a remote computer connected to the host computer which is indicative of a request for provision of the key credential information is detected. Using the

secure logic circuitry, a message prompting a user for providing the key credential information is generated. Using a secure user interface connected to the secure logic circuitry, the key credential information is received from the user and provided to the secure logic circuitry. Using the secure logic circuitry, the key credential information is provided to the remote computer absent processing using circuitry of the host computer.

The advantage of the present invention is that it provides a system for secure provision of key credential information to a server via an un-trusted computer.

A further advantage of the present invention is that it provides a system for secure provision of key credential information that is easily installed in an existing computer system.

BRIEF DESCRIPTION OF THE DRAWINGS

A preferred embodiment of the present invention is described below with reference to the accompanying drawings, in which:

Figures 1A and 1B are simplified block diagrams of a system for secure provision of key credential information according to a preferred embodiment of the present invention; and,

Figure 2 is a simplified flow diagram of a method for secure provision of key credential information according to a preferred embodiment of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENT

Unless defined otherwise, all technical and scientific terms used herein have the same meaning as commonly understood by one of ordinary skill in the art to which the invention belongs. Although any methods and materials similar or equivalent to those described herein can be used in the practice or testing of the present invention, the preferred methods and materials are now described.

While the description of the preferred embodiments herein below is with reference to an Internet connection for sake of simplicity, it will become evident to those skilled in the art that the embodiments of the invention are not limited thereto, but are also applicable for use with various other networks such as, for example, corporate networks or university networks.

Referring to Figures 1A and 1B, a system for secure provision of key credential information 100 according to a preferred embodiment of the invention is provided. A user's Personal Computer (PC) or workstation 102 is connected via a communication network 114 such as, for example, the Internet, to a remote computer 116, for example, a server of an Internet based booking center or vendor. Typically, computers such as PCs and workstations communicate with the communication network 114 via a Network Interface Card (NIC) 118 which is connected to a motherboard 110 comprising a Central Processing Unit (CPU) 106 via an internal bus system. The user typically interacts with the computer 102 using key board 112 for providing information and commands to the CPU 106 and monitor 104 for visually receiving information, for example, in a graphical fashion.

The system for secure provision of key credential information 100 enables a user to communicate key credential information to the server 116 such that a malware having, for example, a surreptitious key logger capability, resident in the computer's CPU 106 or motherboard 110 is not able to see the provided key credential information.

The system for secure provision of key credential information 100 preferably comprises a NIC 118 having secure logic circuitry 120 connected to ports 130, 132, and 134. The ports 132 and 134 are connected to the communication network 114 and the internal bus system of the computer 102, respectively. The secure logic circuitry 120 comprises, for example, a processor 136 and memory 138 having executable commands stored therein for execution on the processor 136. The secure logic circuitry 120 scans messages received from the server 116 for detecting a message which is indicative of a request for provision of the key credential information. Typically, when a user attempts to invoke a service on a remote network resource, the server then sends a request for credentials message to the computer 102. For example, in conventional web browsing operations the CPU 106 of the computer 102 sends a HTTP GET message to the server 116 specifying a server resource and the server 116 replies with a HTTP 401

Authorization Required message with an embedded realm-title such as "Some-Service Login" to alert the user to exactly which set of key credentials are required for the requested resource.

When the secure logic circuitry 120 encounters a "request for key credentials" message the request is not passed to the computer motherboard 110 – as is done using conventional technology - but instead is passed to a secure user interface 124, 126 connected to the secure logic circuitry 120 via the port 130. The secure user interface comprises, for example, a secure keyboard 126 for receiving the key credential information from the user and a secure display 124 for displaying a message for prompting the user for provision of the key credential information. Alternatively, the secure user interface comprises a touch screen. The secure user interface is deployed, for example, as a peripheral device connected to the port 130 via cable 122. Alternatively, wireless communication is enabled between the secure logic circuitry 120 and the secure user interface 124, 126 using, for example, RF or infrared signal transmission techniques. For example, for common web browsing the secure logic circuitry 120 scans for messages coming from remote port 80 that contain the HTTP 401 message. More generally, a dedicated internet protocol is used to handle credentials for more general services or the secure logic circuitry 120 scans for authentication for each type of internet protocol, e.g. POP on port 132. The secure logic circuitry 120 generates a message for prompting the user for provision of the key credential information which is then transmitted to the secure display 124 for alerting the user. Optionally, an audio alert is generated using, for example, a loudspeaker disposed in the secure user interface. For example, for a common web browsing situation, the secure display shows the embedded realm title such as "Some-Service Login".

Optionally, the secure logic circuitry interrupts communication between the keyboard and the motherboard, for example, simultaneously when the message for prompting the user for provision of the key credential information is displayed.

Optionally, keyboard 126 can be enhanced with a second non-secured keyboard-to-PC connection link (not shown) that can transmit keystrokes from the enhanced keyboard 126 to the PC motherboard 110 in a non-secure mode, this optional enhanced keyboard 126 additionally having a user-activatable switch 128 that, when activated, temporarily blocks future transmission via the second non-secured keyboard-to-PC connection link to halt any typed keystrokes

provided from the keyboard from reaching the motherboard 110, and when activated, additionally temporarily allowing future transmission of data from the enhanced keyboard 126 to the NIC 118 via cable 122 or such other manner known to a person skilled in the art. This eliminates the requirement for the PC user to have separate secure and non-secure keyboards.

The user enters the required key credential information which is then sent to the secure logic circuitry 120 via cable 122. Upon receipt, the secure logic circuitry 120 provides the key credential information to the remote computer 116 absent processing using the motherboard 110, for example, by generating a reply message with the key credential information contained therein. Once the key credential information has been received, conventional communication and operation proceeds. For the common web browsing situation the secure logic circuitry 120 additionally keeps track of outgoing HTTP GET requests, because within the HTTP protocol, an authorization message is supplied by retrying the original HTTP GET request with an additional Authorization field added that contains the key credential information.

As is evident, there are numerous variants for coding the key credential information. For example, the HTTP protocol defines a low security Basic mode, where the key credential information is transmitted over the network using a base-64 transfer encoding. HTTP also includes a Digest based authentication mechanism, whereby the HTTP 401 message also contains a one-time unique server supplied "salt" value. In this authentication technique, the authentication reply is a specified hash computation of the user key credential information and the "salt" value, for which the server evaluates the correctness. Using this technique, a network based eavesdropper is not able to recover the key credential information. Of course, there are numerous other methods for encoding the key credential information using various encryption techniques. The secure logic circuitry 120 is adaptable to perform these various encoding techniques in a straightforward manner.

The system for secure provision of key credential information 100 is easily installed, for example, in the form of a NIC, into an existing insertion slot of a computer such as a PC or workstation with the secure user interface being connected thereto, allowing retrofitting of existing computer systems in a simple fashion.

Referring to Figure 2, a simplified flow diagram of a method for secure provision of key credential information according to a preferred embodiment of the invention is provided. The method is implemented using the system 100 described above. At 10, using the secure logic circuitry 120 disposed in the host computer 102 messages received from the remote computer 116 are scanned for detecting – 12 - a message received from the remote computer 116 which is indicative of a request for provision of key credential information. Upon detection of the message, the secure logic circuitry generates a message prompting a user for providing the key credential information – 14. Optionally, the secure logic circuitry interrupts – 16 - communication between circuitry 110 of the host computer 102 and the remote computer 116 to increase security. At 18, transmission of keystroke signals to the circuitry 110 of the host computer 102 from a keyboard 112 connected to the host computer 102 is interrupted. The interruption is performed, for example, when a same keyboard connected to the motherboard 110 and to the secure logic circuitry 120 is used. For example, the user presses a toggle switch disposed on the keyboard prior provision of the key credential information. Alternatively, the interruption is performed automatically, using the secure logic circuitry 120. Optionally, the interruption is also performed when two separate keyboards or a touch screen are employed to prevent accidental use of the keyboard connected to the motherboard 110 for provision of the key credential information by the user.

At 20, the secure logic circuitry generates display data for displaying the message prompting the user which is then displayed – 22- using the secure display 124. Using the secure user interface connected to the secure logic circuitry 120, the key credential information is received from the user and provided to the secure logic circuitry 120, at 24. Using the secure logic circuitry 120, the key credential information is encoded – 26 – using one of various available encoding techniques for providing the key credential information in an obfuscated fashion. The secure logic circuitry 120 then sends – 28 - the key credential information to the remote computer 116 absent processing using circuitry 110 of the host computer 102.

After provision of the key credential information to the remote computer 116 communication between the circuitry 110 of the host computer 102 and the remote computer 116 is enabled – 30 – as well as transmission of keystroke signals from the keyboard to the circuitry 110 of the host computer 102, at 32.

It is understood that in the preferred embodiment of the present invention, the NIC of the present invention would not incorporate or utilize a conventional packet sniffer function that would capture the secure credential packets being transmitted therethrough (to mitigate the risk that malware could locate and acquire such data from the NIC).

It is also understood that, in the case of a laptop computer, a NIC of the present invention may be provided which is physically separate from, and connectable to the laptop by way of, for example, a USB port or other interface on the laptop, in a manner known to a person skilled in art (network access to and from laptop thereafter being provided by way of the NIC of the present invention).

The present invention has been described herein with regard to preferred embodiments. However, it will be obvious to persons skilled in the art that a number of variations and modifications can be made without departing from the scope of the invention as described herein.

THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A system for secure provision of key credential information over a communications network from a user to a remote computer, for use with a host computer comprising a motherboard and a communications network interface for sending and receiving communications to the remote computer through the communications network, the system comprising:

(a) secure logic circuitry configured for performing the following steps absent processing using the motherboard: I) communicating with a secure user interface; II) communicating with the remote computer through the communications network; III) detecting a request by the remote computer for key credential information; and, IV) after detecting the request, interrupting any passage of key credential information to the motherboard and, while passage of key credential information to the motherboard is interrupted: (i) generating a message for prompting a user for provision of the key credential information; (ii) obtaining the key credential information through the secure user interface; and, (iii) sending the obtained key credential information to the remote computer through the communications network interface; and,

(b) a secure user interface connected to the secure logic circuitry and configured for using the generated message to alert the user to provide the key credential information, receiving the key credential information from the user and sending the key credential information to the secure logic circuitry.

2. A system according to claim 1 wherein the request by the remote computer is associated with a resource of the remote computer and comprises resource identifying information identifying the resource; the message sent to the secure user interface by the secure logic circuitry comprises the resource identifying information; and, the alert to the user by the secure user interface is configured for providing the resource identifying information to the user.

3. A system according to claim 2 wherein the secure user interface comprises a display for displaying the alert for prompting the user to provide the key credential information; and, a keyboard for the user to provide the key credential information.

4. A system according to claim 3 wherein the display and keyboard of the secure user interface comprise a touch screen and/or the secure user interface is configured for alerting the user by audio means.

5. A system according to any one of claims 1 to 4 wherein the secure user circuitry is configured for encrypting and decrypting communications with the remote computer.

6. A system according to any one of claims 1 to 5 wherein a host user interface is normally operative for communication with the motherboard and the secure logic circuitry is further configured for disabling communication between the host user interface and motherboard before sending the prompt to the secure user interface, and for re-enabling communication between the host user interface and the motherboard after sending the obtained key credential information.

7. A system according to any one of claims 1 to 6 wherein a network interface card comprises the secure logic circuitry .

8. A system according to claim 7 wherein the secure user interface comprises a peripheral device configured for connecting to the network interface card.

9. A system according to any one of claims 1 to 8 wherein the secure logic circuitry comprises a processor and memory, the memory having executable commands stored therein for execution on the processor.

10. A system according to any one of claims 1 to 9, wherein the secure user interface notifies the user of the received key credential information before sending it to the secure logic circuitry.

11. A system according to claim 3, wherein the keyboard of the secure user interface is an enhanced keyboard configured for connection to a host user interface of the host computer by means of a user-activatable switch.

12. A system according to any one of claims 1 to 11 wherein the remote computer comprises a server, the resource is an Internet service and the request for and sending of the key credential information are for a transaction pertaining to the Internet service.

13. A method for secure provision of key credential information over a communications network from a user to a remote computer, for use with a host computer comprising a motherboard and a communications network interface for sending and receiving communications to the remote computer through the communications network, the method comprising:

(a) detecting a request by the remote computer for key credential information; and,

(b) after detecting the request, interrupting any passage of key credential information to the motherboard and, while passage of key credential information to the motherboard is interrupted : (i) by secure logic circuitry and absent processing using the motherboard, generating a message for prompting a user for provision of the key credential information; (ii) by secure logic circuitry and based on the generated message, alerting the user to provide the key credential information; and, (iii) by the secure logic circuitry and absent processing using the motherboard, obtaining the key credential information from the user and sending the obtained key credential information to the remote computer through the communications network interface.

14. A method according to claim 13 whereby the request by the remote computer is associated with a resource of the remote computer and comprises resource identifying information identifying the resource; the generated message comprises the resource identifying information; and, the alerting includes providing the resource identifying information to the user.

15. A method according to claim 14 whereby a host user interface is normally operative for communication between the user with the motherboard, the method further comprising the secure logic circuitry disabling communication between the host user interface and motherboard by the secure logic circuitry before alerting the user to provide the key credential information and re-enabling communication between the host user interface and the motherboard after sending the obtained key credential information.

16. A system for secure provision of key credential information provided by a user of the host computer against any malware resident in a motherboard of the host computer, the host computer configured for network communications with a remote computer through a communications network interface, the system comprising secure logic circuitry for use with the host computer and a secure user interface for use by the user, wherein:

(a) the secure logic circuitry is configured for:

(i) detecting a request message received from the remote computer indicative of a request for provision of the key credential information;

(ii) generating a prompt message for prompting the user to provide the key credential information;

(iii) transmitting the prompt message to the secure user interface;

(iv) receiving the key credential information from the secure user interface; and,

(v) providing the received key credential information to the remote computer absent processing using the motherboard; and,

(b) the secure user interface is configured for connection to the secure logic circuitry and, for:

(i) receiving the key credential information from the user; and,

(ii) providing the key credential information to the secure logic circuitry.

17. A system for secure provision of key credential information as defined in claim 16 wherein the request message is associated with a resource of the remote computer and comprises a HTTP 401 Authorization Required message with an embedded realm-title.

18. A system for secure provision of key credential information as defined in claim 15 wherein the secure user interface comprises: (i) a secure display for displaying the embedded realm-title to alert the user as to which key credentials are required for the resource; and, (ii) a secure keyboard for use by the user for providing the key credential information.

19. A system for secure provision of key credential information as defined in claim 18 wherein the secure display and secure keyboard comprise a touch screen.

20. A system for secure provision of key credential information as defined in claim 18 or 19 wherein the secure user interface is configured for alerting the user by audio means.

21. A system for secure provision of key credential information as defined in any of claims 17 to 20 wherein the secure logic circuitry is adaptable to perform encoding of the key credential information using an encryption technique.

22. A system for secure provision of key credential information as defined in any one of claims 16 to 21 wherein a host computer keyboard connected to the host computer is normally operative for use by the user to provide communications in a non-secure mode to a central processing unit of the motherboard and the secure logic circuitry is configured for interrupting said non-secure mode communications from the host computer keyboard to the motherboard prior to provision of the key credential information by the user, and for re-enabling said non-secure mode communications

from the host computer keyboard to the motherboard after providing the key credential information to the remote computer.

23. A system for secure provision of key credential information as defined in any one of claims 16 to 22 wherein the secure logic circuitry is configured for being disposed in the host computer.

24. A system for secure provision of key credential information as defined in any one of claims 16 to 23 wherein the secure logic circuitry is placed on a network interface card and the secure user interface is provided as a peripheral device connected to the network interface card.

25. A system for secure provision of key credential information as defined in any one of claims 16 to 24 wherein the secure logic circuitry comprises a processor and memory, the memory having executable commands stored therein for execution on the processor.

26. A system for secure provision of key credential information as defined in any one of claims 16 to 25, wherein a same enhanced keyboard is connected to both the motherboard and to the secure logic circuitry and is activatable by the secure logic circuitry to operate in either: (i) a non-secure mode to transmit keystroke signals from the enhanced keyboard to the motherboard; or, a secure mode to interrupt transmission of keystroke signals from the enhanced keyboard to the motherboard, and the secure logic circuitry comprises activating means for activating the mode of operation of the enhanced keyboard to the secure mode prior to receiving the key credential information from the user and for activating the mode of operation of the enhanced keyboard to the non-secure mode after the secure logic circuitry has provided the key credential information to the remote computer.

27. A system for secure provision of key credential information as defined in claim 26 wherein the activating means is provided by a user-activatable switch or by the secure logic circuitry configured for automatically activating the mode of operation.

28. A system for secure provision of key credential information as defined in claim 17 wherein the remote computer comprises a server and the resource is an Internet service.

29. A method for secure provision of key credential information by a user of a host computer against malware resident in a motherboard of the host computer, the host computer configured for network communications with a remote computer through a communications network interface, the method comprising:

(a) providing a secure user interface configured for receiving the key credential information from the user;

(b) using a secure logic circuitry disposed in a host computer and connected to the secure user interface, detecting a request message received from the remote computer indicative of a request for provision of the key credential information;

(c) using the secure logic circuitry, generating a prompt message for prompting the user for provision of the key credential information using the secure user interface;

(d) using the secure logic circuitry, transmitting the prompt message to the secure user interface;

(e) using the secure user interface, receiving the key credential information from the user and providing the key credential information to the secure logic circuitry; and,

(f) using the secure logic circuitry, providing the key credential information to the remote computer absent processing using circuitry of the motherboard.

30. A method as defined in claim 29 whereby the request message from the remote computer is associated with a resource of the remote computer and comprises a HTTP 401 Authorization Required message with an embedded realm-title, and the embedded realm-title is provided to the user to alert the user as to which key credentials are required for the resource.

31. A method as defined in claim 29 or 30 whereby a host user interface is normally operative for use by the user to provide communications in a non-secure mode from the user to the motherboard, the method further comprising interrupting the non-secure mode communications between the host user interface and the motherboard before the alerting the user to provide the key credential information and re-enabling the non-secure mode communications between the host user interface and the motherboard after providing the received key credential information to the remote computer.

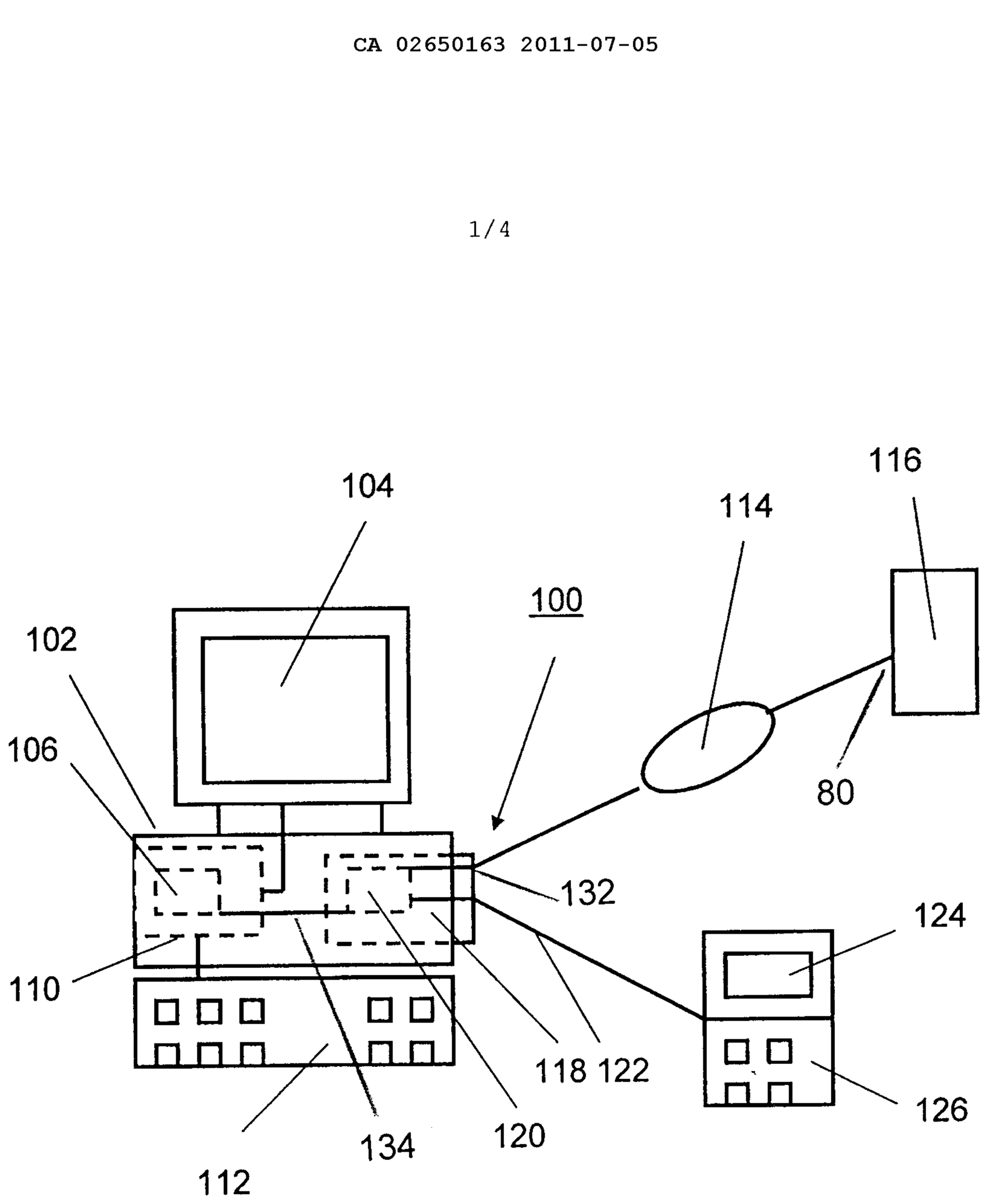


Figure. 1A

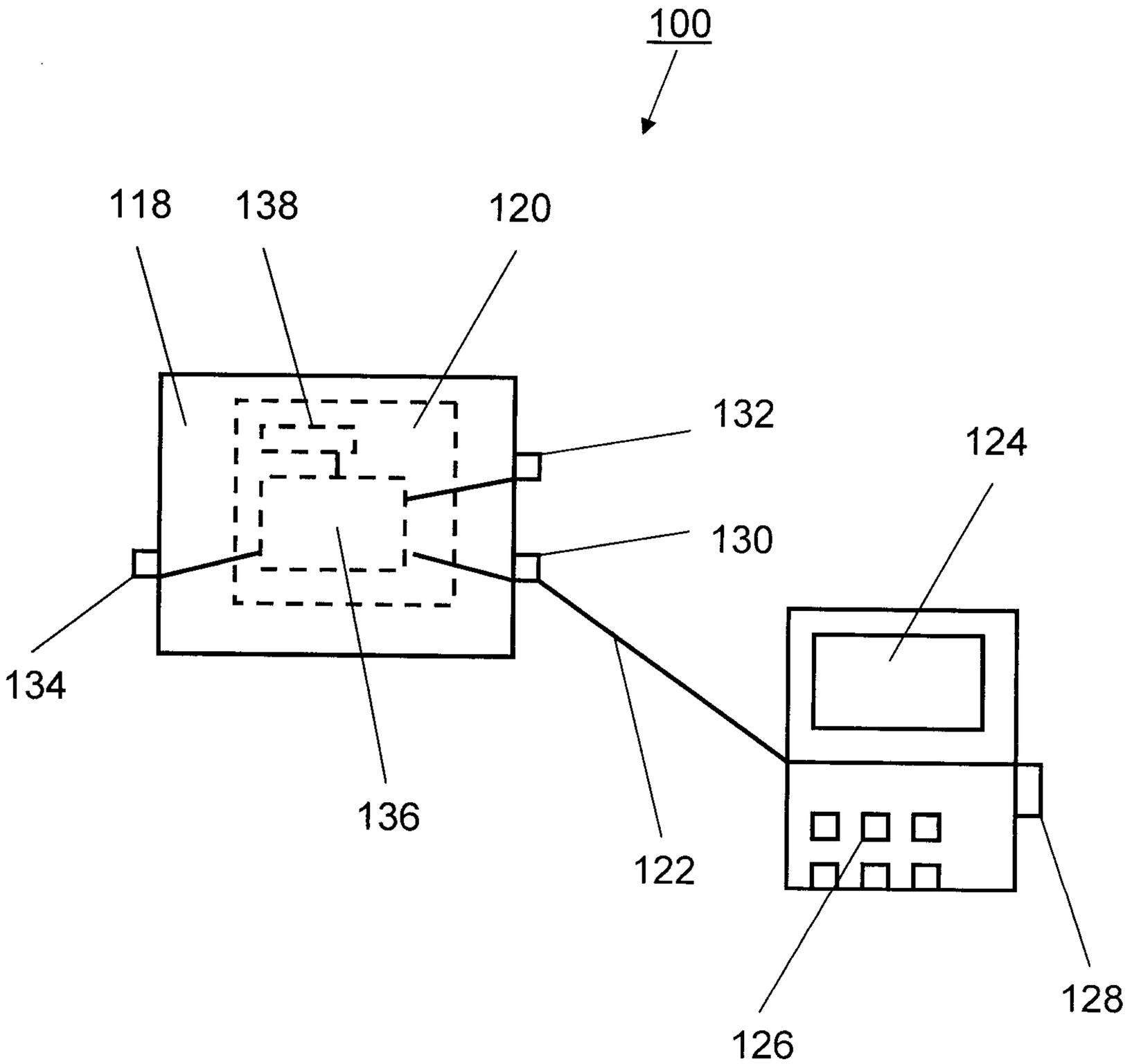


Figure. 1B

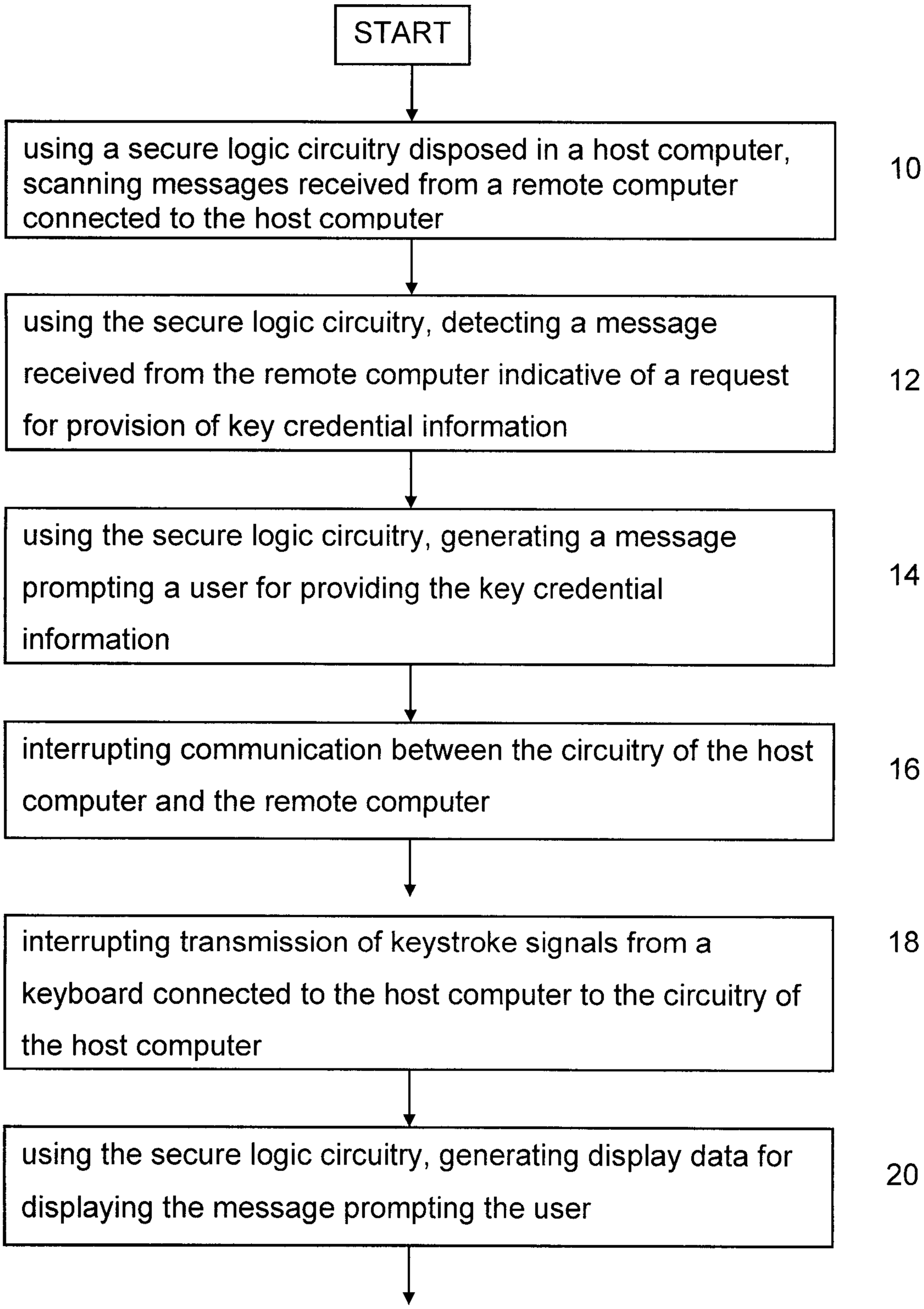

START
using a secure logic circuitry disposed in a host computer, scanning messages received from a remote computer connected to the host computer
10
using the secure logic circuitry, detecting a message received from the remote computer indicative of a request for provision of key credential information
12
using the secure logic circuitry, generating a message prompting a user for providing the key credential information
14
interrupting communication between the circuitry of the host computer and the remote computer
16
interrupting transmission of keystroke signals from a keyboard connected to the host computer to the circuitry of the host computer
18
using the secure logic circuitry, generating display data for displaying the message prompting the user
20

Fig. 2

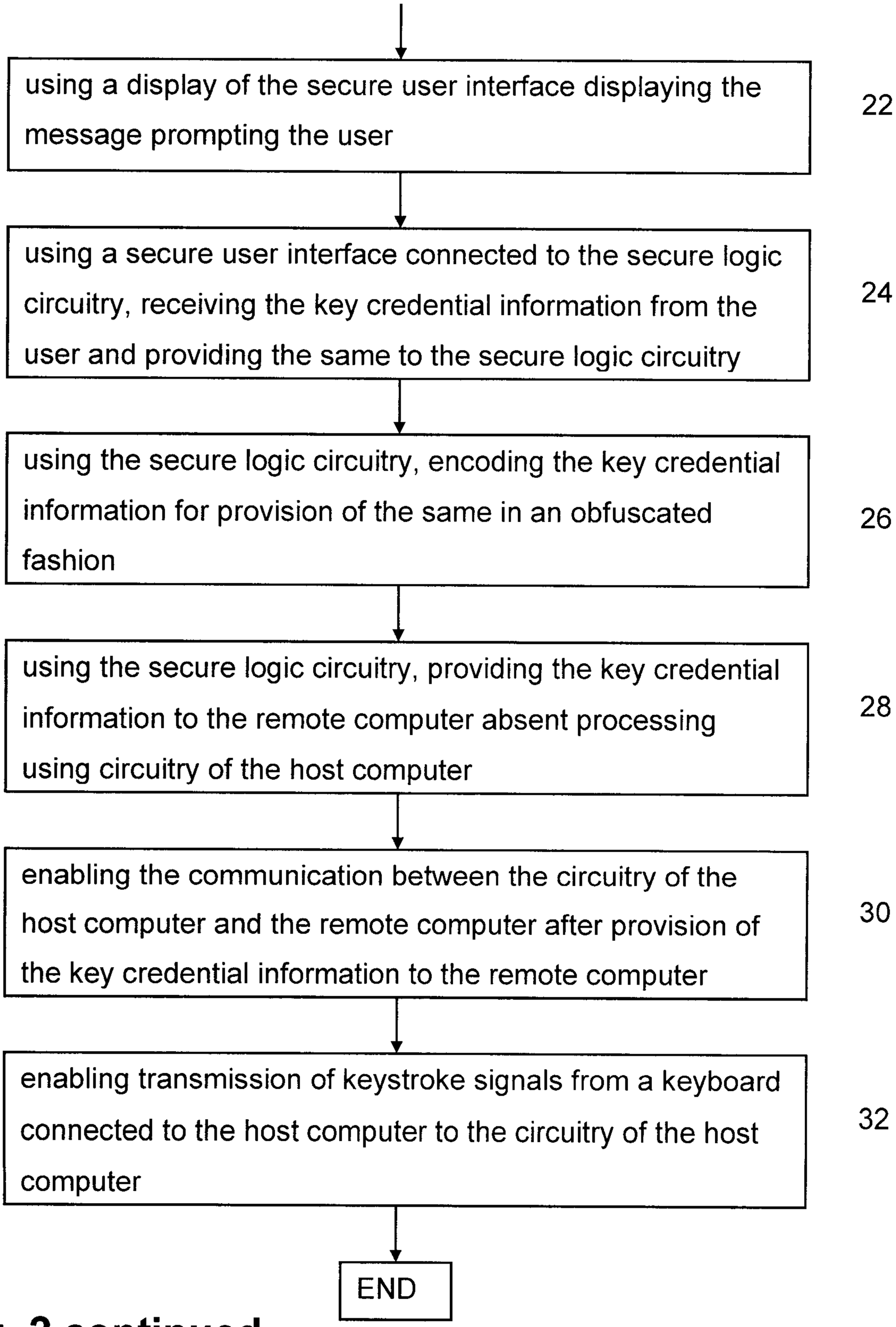
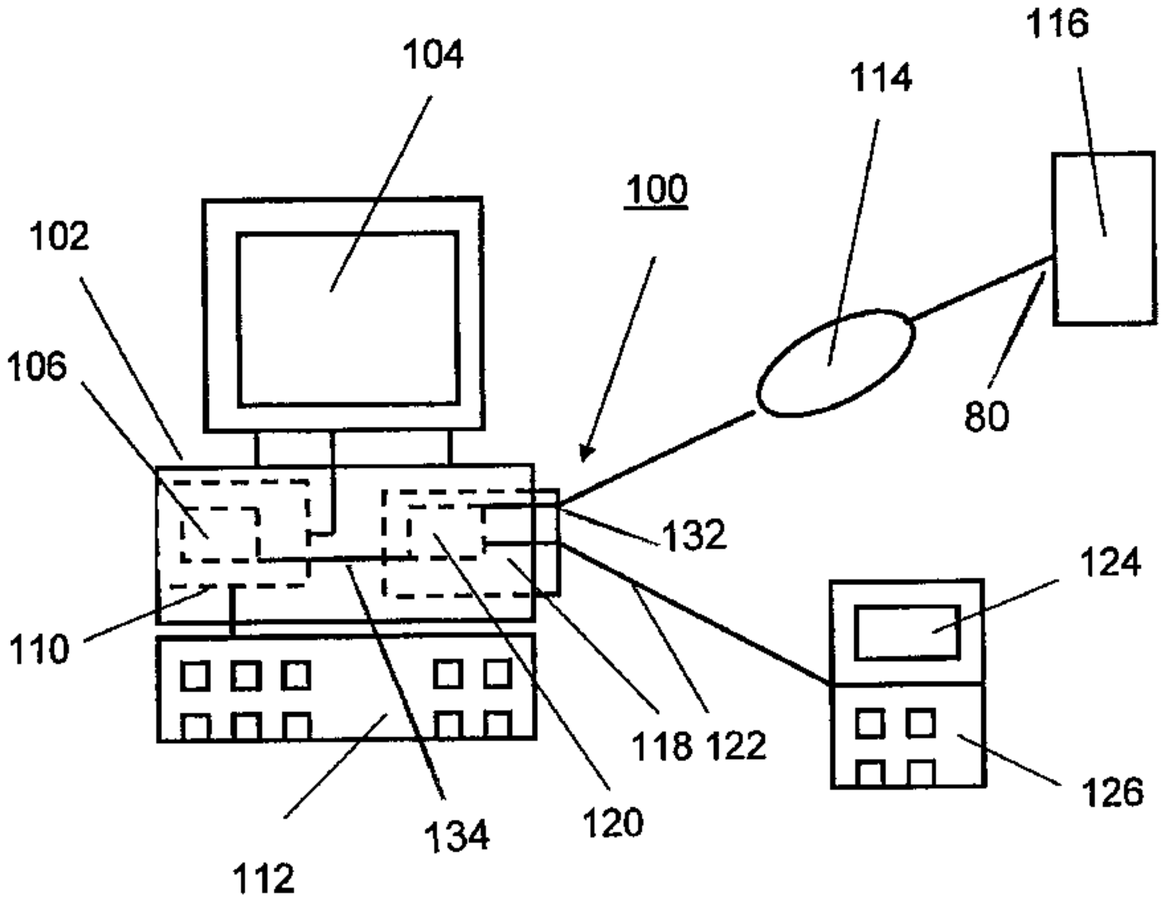
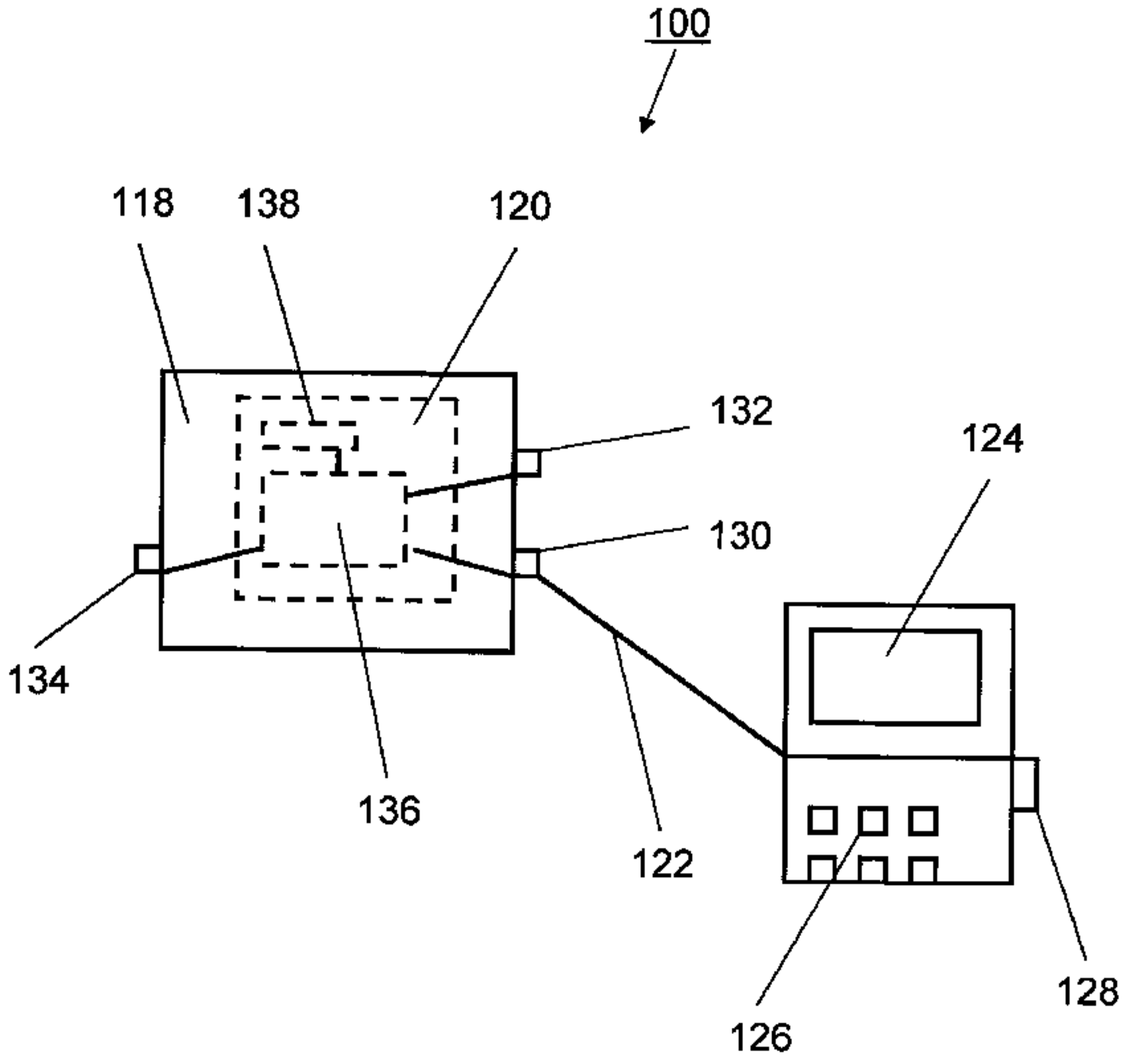


Fig. 2 continued


104
116
114
100
102
106
80
132
124
110
118
122
126
134
120
112

A


100
118
138
120
132
124
130
134
136
122
126
128

B