(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 August 2011 (04.08.2011)

PCT

(10) International Publication Number
WO 2011/094616 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *G06F 21/00* (2006.01)

(21) International Application Number:
PCT/US2011/023028

(22) International Filing Date:
28 January 2011 (28.01.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

61/282,378	29 January 2010 (29.01.2010)	US
61/282,478	17 February 2010 (17.02.2010)	US
61/282,503	22 February 2010 (22.02.2010)	US
61/282,861	12 April 2010 (12.04.2010)	US
61/344,018	7 May 2010 (07.05.2010)	US
61/457,184	24 January 2011 (24.01.2011)	US
13/014,201	26 January 2011 (26.01.2011)	US

(72) Inventor; and
(71) Applicant : **ELLIS, Frampton, E.** [US/US]; P. O. Box 1029, Jasper, FL 32052 (US).

(74) Agent: **GARRETT, Arthus, S.**; Finnegan, Henderson, Farabow, Garrett & Dunner,L.L.P., 901 New York Avenue, NW, Washington, DC 20001-4413 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) **Title**: THE BASIC ARCHITECTURE FOR SECURE INTERNET COMPUTERS

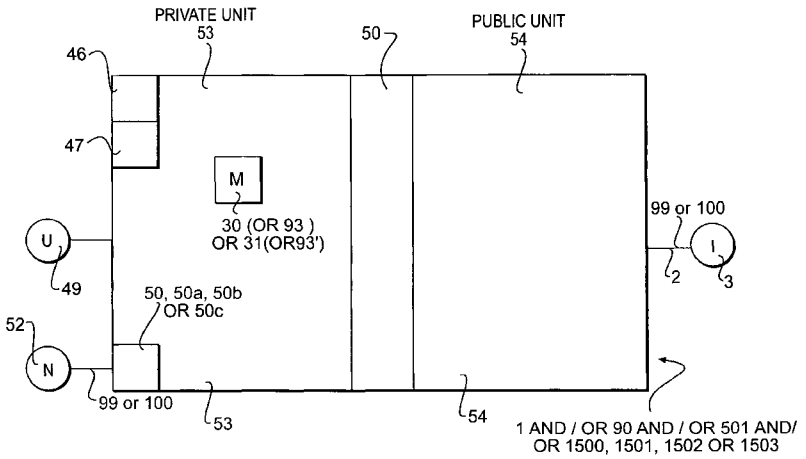

FIG. 1

(57) **Abstract**: A method or apparatus for a computer or microchip with one or more inner hardware-based access barriers or firewalls that establish one or more private units disconnected from a public unit having connection to the Internet, and one or more of the private units have a connection to one or more secure non-internet-connected private networks for personal and/or local administration. The hardware-based access barriers include a single out-only bus and/or another in-only bus with a single on/off switch and/or both buses, each with a single on/off switch. The hardware-based access barriers can be positioned successively between an outer private unit, an intermediate more private unit, an inner most private unit, and the public unit, and each private unit can be configured for a separate connection to a separate network of computers that excludes the Internet.

WO 2011/094616 A1

THE BASIC ARCHITECTURE FOR SECURE INTERNET COMPUTERS

Applicant claims the right to priority based on U.S. Provisional Patent Application No. 61/282,378, filed January 29, 2010; U.S. Provisional Patent Application No. 61/282,478, filed February 17, 2010; U.S. Provisional Patent Application No. 61/282,503, filed February 22, 2010; U.S. Provisional Patent Application No. 61/282,861, filed April 12, 2010; U.S. Provisional Patent Application No. 61/344,018, filed May 7, 2010; and U.S. Provisional Patent Application No. _____ (GNC33PA), filed January 24, 2011.

Applicant also claims the right to priority based on U.S. Nonprovisional Patent Application No. 13/014,201, filed January 26, 2011. The contents of all of these provisional and nonprovisional patent applications are hereby incorporated by reference in their entirety.

BACKGROUND OF THE INVENTION

This invention relates to any computer, such as a personal computer and/or microchip or wafer with an inner hardware-based access barrier or firewall that establishes a private unit or zone that is disconnected from a public unit or zone having connection to a network of computers, such as the Internet, as well as the private unit having one or more connections to one or more secure non-Internet-connected private networks for personal and/or local administration of the computer and/or microchip.

More particularly, this invention relates to a computer and/or microchip with an inner hardware-based access barrier or firewall separating the private unit that is not connected to the Internet from a public unit connected to the Internet, the private and

public units being connected only by a hardware-based access barrier or firewall in the form of a secure, out-only bus or wireless connection. Even more particularly, this invention relates to the private and public units also being connected by an in-only bus that includes a hardware input on/off switch or equivalent signal interruption mechanism, including an equivalent circuit on a microchip or nanochip. Still more particularly, this invention relates to the private and public units being connected by an output on/off switch or microcircuit equivalent on the secure, out-only bus.

In addition, this invention relates to a computer and/or microchip that is connected to a another computer and/or microchip, the connection between computers made with the same hardware-based access barriers or firewalls including the same buses with on/off switches described above.

Finally, this invention relates to a computer and/or microchip with hardware-based access barriers or firewalls used successively between an outer private unit, an intermediate more private unit, an inner most private unit, and the public unit, also including Faraday Cage protection from external electromagnetic pulses.

By way of background, traditionally computer security has been based primarily on conventional firewalls that are positioned externally, between the computer and the external network. Such conventional firewalls provide a screening or filtering function to identify and block incoming network malware. But because of their functionally external position, conventional firewalls must allow entry to a significant amount of incoming traffic, so they must perform perfectly, an impossibility, or at least some malware inherently gets into the computer. Once in, the von Neumann architecture of current computers provides only software protection, which is inherently vulnerable to malware attack, so existing computers are essentially indefensible from successful attack from the Internet, which

has provided an easy, inexpensive, anonymous, and effective means for the worst of all hackers worldwide to access any connected computer.

SUMMARY OF THE INVENTION

Therefore, computers cannot be successful defended without inner hardware or firmware-based access barriers or firewalls that, because of their internal position, can be designed to function as access barrier or blockers rather than as general filters. This is a critical distinction. An Internet filter has to screen the entire Internet, which is without measure in practical terms and constantly changing, an impossible task. In contrast, an access barrier or blocker to an inner protected area of a computer can strictly limit access to only an exception basis. So, in simple terms, a conventional firewall generally grants access to all Internet traffic unless it can be identified as being on the most current huge list of malware; in contrast, an inner access barrier or blocker can simply deny access to all except to a carefully selected and very short and conditioned list of approved sources or types of traffic.

Such a much simpler and achievable access blocking function allowing for a much simpler and efficient mechanism for providing the function. Whereas a conventional but imperfect firewall involves highly complicated hardware with millions of switches and/or firmware and/or software with millions of bits of code, the hardware-based access barriers described in this application require as little as a single simple one-way bus and/or another simple one-way bus with just a single switch and/or both simple buses, each with just a single switch. This extraordinarily tiny amount of hardware is at the absolute theoretical limit and cannot be less.

With this new and unique approach, computers and microchips can be simply and

effectively defended from Internet attack with one or more private, protected hardware-based zones inside the computer, any of which can be personally or locally administrated by a separate and secure non-Internet private network.

This application hereby expressly incorporates by reference in its entirety U.S. Patent Application No. 10/684,657 filed October 15, 2003 and published as Pub. No. US 2005/0180095 A1 on August 18, 2005 and U.S. Patent Application No. 12/292,769 filed November 25, 2008 and published as Pub. No. US 2009/0200661 A1 on August 13, 2009.

Also, this application hereby expressly incorporates by reference in its entirety U.S. Patent Application No. 10/802,049 filed March 17, 2004 and published as Pub. No. US 2004/0215931 A1 on October 28, 2004 and U.S. Patent Application No. 12/292,553 filed November 20, 2008 and published as Pub. No. US 2009/0168329 A1 on July 2, 2009.

Finally, this application hereby expressly incorporates by reference in its entirety U.S. Patent No. 6,167,428 issued 26 December 2000, U.S. Patent No 6,725,250 issued 20 April 2004, U.S. Patent No. 6,732,141 issued 4 May 2004, U.S. Patent No. 7,024,449 issued 4 April 2006, U.S. Patent No. 7,035,906 issued 25 April 2006, U.S. Patent No. 7,047,275 issued 16 May 2006, U.S. Patent No 7,506,020 issued 17 March 2009, U.S. Patent No. 7,606,854 issued 20 October 2009, U.S. Patent No. 7,634,529 issued 15 December 2009, U.S. Patent No. 7,805,756 issued 28 September 2010, and 7,814,233 issued 12 October 2010.

Definitions and reference numerals are the same in this application as in the above incorporated '657, '769, '049 and '553 U.S. Applications, as well as in the above incorporated '428, '250, '141, '449, '906, '275, '020, '854, '529, '756, and '233 U.S. Patents.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows any computer, such as a personal computer 1 and/or microchip 90 (and/or 501) with an inner hardware-based access barrier or firewall 50 establishing a Private Unit or zone 53 of the computer or microchip that is disconnected from a Public Unit or zone 54 that is connected to the Internet 3 (and/or another, intermediate network 2). Fig. 1 also shows an example embodiment of the Private Unit 53 having at least one connection to at least one private or secure non-Internet-connected network 52 for personal or local administration of the personal computer 1 and/or microchip 90 (and/or 501) and/or silicon wafer 1500 (or portion 1501, 1502, and/or 1503), or graphene equivalent. The number and placement of the non-Internet-connected networks 52 is optional.

Figure 2 shows an example embodiment of a personal computer 1 and/or microchip 90 (and/or 501) with an inner hardware-based access barrier or firewall 50 separating a Private Unit 53 disconnected from the Internet 3 and a Public Unit 54 connected to the Internet 3, the Private Unit 53 and Public Unit 54 connected only by a hardware-based access barrier or firewall 50a, for example in the form of a secure, out-only bus (or wire) or channel 55 (or in an alternate embodiment, a wireless connection, including radio or optical).

Figure 3 is a similar example embodiment to that shown in Figure 2, but with the Private Unit 53 and Public Unit 54 connected by a hardware-based access barrier or firewall 50b example that also includes an in-only bus or channel 56 that includes a hardware input on/off switch 57 or equivalent function signal interruption mechanism, including an equivalent functioning circuit on a microchip or nanochip.

Figure 4 is a similar example embodiment to that shown in Figure 2 and 3, but with Private Unit 53 and Public Unit 54 connected by a hardware-based access barrier or firewall 50c example that also includes an output on/off switch 58 or microcircuit equivalent on the secure, out-only bus or channel 55.

Figure 5 shows an example embodiment of any computer such as a first personal computer 1 and/or microchip 90 (and/or 501) that is connected to a second computer such as a personal computer 1 and/or microchip 90 (and/or 501), the connection between computers made with the same hardware-based access barrier or firewall 50c example that includes the same buses or channels with on/off switches or equivalents as Figure 4.

Figure 6 shows an example embodiment of a personal computer 1 and/or microchip 90 (and/or 501) similar to Figures 23A and 23B of the '657 Application, which showed multiple access barriers or firewalls 50 with progressively greater protection, but with hardware-based access barriers or firewalls 50c, 50b, and 50a used successively from a inner private unit 53, to an intermediate more private unit 53^1, and to an inner most private unit 53^2, respectively.

Figures 7-14 are additional architectural embodiment examples of the use of hardware-based access barriers or firewalls 50a, 50b, and 50c.

Figs. 15 and 16 illustrate methods in accordance with the present disclosure.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Figures 1-4, 6, 8-14 all show useful architectural example embodiments of any computer or microchip, including a personal computer 1 and/or microchip 90 (and/or 501) or silicon (or graphene) wafer 1500 (or wafer portion 1501, 1502, and/or 1503) with an inner hardware-based access barrier or firewall 50 establishing a secure Private Unit 53

that is directly controlled by a user 49 (local in this example) and disconnected by hardware from a Public Unit 54 that is connected to the Internet 3 and/or another, intermediate network 2; the connection of the computer 1 (and/or 90 and/or 501) to the network 2 and/or Internet 3 can be wired 99 or wireless 100.

Hardware-based access barrier or firewall 50 (or 50a, 50b, or 50c) as used in this application refers to an access barrier that includes one or more access barrier or firewall-specific hardware and/or firmware components. This hardware and/or firmware configuration is in contrast to, for example, a computer firewall common in the art that includes only software and general purpose hardware, such as an example limited to firewall-specific software running on the single general purpose microprocessor or CPU of a computer.

The Internet-disconnected Private Unit 53 includes a master controlling device 30 for the computer PC1 (and/or a master controller unit 93 for the microchip 90 and/or 501) that can include a microprocessor or processing unit and thereby take the form of a general purpose microprocessor or CPU, for one useful example, or alternatively only control the computer as a master controller 31 or master controller unit 93'. The user 49 controls the master controlling device 30 (or 31 or 93 or 93') located in the Private Unit 53 and controls both the Private Unit 53 at all times and any part or all of the Public Unit 54 selectively, but can peremptorily control any and all parts of the Public Unit 54 at the discretion of the user 49 through active intervention or selection from a range of settings, or based on standard control settings by default.

More particularly, Figure 1 shows a useful example of an optional (one or more) secure private non-Internet-connected network 52 for personal or local administration of the Private Unit 53. Wired 99 connection offers superior security generally, but wireless

100 connection is a option, especially if used with a sufficiently high level of encryption and/or other security measures, including low power radio signals of high frequency and short range and/or directional. Access from the private non-Internet-connected network can be limited to only a part of the Private Unit 53 or to multiple parts or to all of the Private Unit 53.

The private non-Internet-connected network 52 (not connected to the Internet either directly or indirectly, such as through another, intermediate network like an Intranet) allows specifically for use as a highly secure network for providing administrative functions like testing, maintenance, or operating or application system updates to any computers (PC1 or microchip 90 or 501) on a local network, such as a business or home network, and would be particularly useful for the example of businesses administering large numbers of local computers, such as network server arrays (especially blades) for cloud applications or supercomputer arrays with a multitude of microprocessors or local clusters. To maximize security, network 52 traffic can be encrypted and/or authenticated, especially if wireless 100.

In addition, in another useful example, a computer (PC1 and/or 90 and/or 501) can be configured so that the private non-Internet-connected network 52 can have the capability to allow for direct operational control of the Private Unit 53, and thus the entire computer, from a remote location, which can be useful for example for businesses operating an array or servers like blades or supercomputers with large numbers of microprocessors or cores.

One or more access barriers or firewalls 50a, 50b, or 50c can be located between the private non-Internet-connected network 52 and the Private Unit 53 provides a useful example of increased security control.

In yet another useful example, a personal user 49 can dock his smartphone (PC1 and/or 90 and/or 501 and/or 1500, 1501, 1502, or 1503) linking through wire or wirelessly to his laptop or desktop computer (PC1 and/or 90 and/or 501 and/or 1500, 1501, 1502, or 1503) in a network 52 connection to synchronize the Private Units 53 of those two (or more) personal computers or perform other shared operations between the Private Units 53. In addition, the Public Units 54 of the user's multiple personal computers can be synchronized simultaneously during the same tethering process, or perform other shared operations between the Public Units 54. Other shared operations can be performed by the two or more linked computers of the user 49 utilizing, for example, two or three or more Private Units 53, each unit with one or more private non-Internet connected networks 52, while two or more Public Units 54 can perform shared operations using one or more other networks 2, including the Internet 3, as shown later in Figure 6.

Also shown in Figure 1 for personal computer PC1 embodiments is an optional removable memory 47 located in the Private Unit 53; the removable memory 47 can be of any form or type or number using any form of one or more direct connections to the Private Unit 53; a thumbdrive or SD card are typical examples, connected to USB, Firewire, or other ports or card slots. Fig. 1 shows as well an optional one or more removable keys 46, of which an access key, an ID authentication key, or an encryption and/or decryption key are examples, also connected to the Private Unit 53 using any form of connection, including the above examples. For microchip 90 (and/or 501) embodiments, wireless connection is a feasible option to enable one or more removable memories 47 or one or more removable keys 46 (or combination of both), particularly for ID authentication and/or access control. In addition, all or part of the Private Unit 53 of a computer PC1 and/or microchip 90 and/or 501 (or wafer 1500, 1501, 1502, or 1501 can

be removable from the remaining portion of the same computer PC1 and/or microchip 90 and/or 501, including the Public Unit 54; the access control barrier or firewall 50 (or 50a and/or 50b and/or 50c) can be removable with the Private Unit 53 or remain with Public Unit 54.

Similarly, Figure 2 shows a useful architectural example embodiment of any computer or microchip, including a personal computer 1 and/or microchip 90 and/or 501 (or wafer 1500, 1501, 1502, or 1503) with an inner hardware-based access barrier or firewall 50 separating a Private Unit 53 that is disconnected by hardware from external networks 2 including the Internet 3 and a Public Unit 54 that is connected to external networks including the Internet 3.

In terms of communication between the two Units in the example shown in Figure 2, the Private Unit 53 and Public Unit 54 are connected only by an inner hardware-based access barrier or firewall 50a in the form of a secure, out-only bus (or wire) or channel 55 that transmits data or code that is output from the Private Unit 53 to be input to the Public Unit 54. The user 49 controls the Private Unit 53-located master controlling device 30 (or 31 or 93 or 93'), which controls all traffic on the secure out-only bus or channel 55. Connections between the user 49 and the master controlling device 30 (or 31 or 93 or 93'), as well as between the master controlling device 30 (or 31 or 93 or 93') and any component controlled by it, can be for example hardwired on a motherboard (and/or executed in silicon on a microchip 90 and/or 501) to provide the highest level of security.

In the example shown in Figure 2, there is no corresponding in-only bus or channel 56 transmitting data or code that is output from the Public Unit 54 to be input to the Private Unit 53. By this absence of any bus or channel into the Private Unit 53, all access from the Internet 3 or intervening network 2 to the Private Unit 53 is completely blocked

on a permanent basis. Another example is an equivalent wireless connection between the two Units would require a wireless transmitter (and no receiver) in the Private Unit 53 and a receiver (and no transmitter) in the Public Unit 54, so the Private Unit 53 can only transmit data or code to the Public Unit 54 and the Public Unit 54 can only receive data or code from the Private Unit 53 (all exclusive of external wireless transmitters or receivers of the PC1 and/or microchip 90 and/or 501).

The Private Unit 53 can include any non-volatile memory, of which read-only memory and read/write memory of which flash memory (and hard drives and optical drives) are examples, and any volatile memory, of which DRAM (dynamic random access memory) is one common example.

An equivalent connection, such as a wireless (including radio and/or optical) connection, to the out-only bus or channel 55 between the two Units 53 and 54 would require at least one wireless transmitter in the Private Unit 53 and at least one receiver in the Public Unit 54, so the Private Unit 53 can transmit data or code to the Public Unit 54 only (all exclusive of external wireless transmitters or receivers of the PC1 and/or microchip 90 and/or 501).

An architecture for any computer or microchip (or nanochip) can have any number of inner hardware-based access barriers or firewalls 50a arranged in any configuration.

Figure 2 also shows an example embodiment of a firewall 50 located on the periphery of the computer 1 and/or microchip 90 (and/or 501) controlling the connection between the computer and the network 2 and Internet 3; the firewall 50 can be hardwire-controlled directly by the master controlling device 30 (or 31 or 93 or 93'), for example.

Figure 3 is a similar useful architectural example embodiment to that shown in Figure 2, but with the Private Unit 53 and Public Unit 54 connected in terms of

communication of data or code by an inner hardware-based access barrier or firewall 50b example that includes a secure, out-only bus or channel 55. The connection between units also includes an in-only bus or channel 56 that is capable of transmitting data or code that is output from the Public Unit 54 to be input into the Private Unit 53, strictly controlled by the master controller 30 (and/or 31 and/or 93 and/or 93') in the Private Unit 53. The in-only bus or channel 56 includes an input on/off switch (and/or microchip or nanochip circuit equivalent) 57 that can break the bus 56 Public to Private connection between Units, the switch 57 being controlled by the Private Unit 53-located master controlling device 30 (or 31 or 93 or 93'), which also controls all traffic on the in-only bus or channel 56; the control can be hardwired.

For one example, the master controller 30 (or 31 or 93 or 93') can by default use the on/off switch and/or micro-circuit (or nano-circuit) equivalent 57 to break the connection provided by the in-only bus or channel 56 to the Private Unit 53 from the Public Unit 54 whenever the Public Unit 54 is connected to the Internet 3 (or intermediate network 2). In an alternate example, the master controller 30 (or 31 or 93 or 93') can use the on/off switch and/or micro or nano-circuit equivalent 57 to make the connection provided by the in-only bus or channel 56 to the Private Unit 53 only when very selective criteria or conditions have been met first, an example of which would be exclusion of all input except when encrypted and from one of only a few authorized (and carefully authenticated) sources, so that Public Unit 54 input to the Private Unit 53 is extremely limited and tightly controlled from the Private Unit 53.

Another example is an equivalent connection, such as a wireless (including radio and/or optical) connection, to the in-only bus or channel 56 with an input on/off switch 57 between the two Units 53 and 54 would require at least one wireless receiver in the

Private Unit 53 and at least one transmitter in the Public Unit 54, so the Private Unit 53 can receive data or code from the Public Unit 54 while controlling that reception of data or code by controlling its receiver, switching it either "on" when the Public Unit 54 is disconnected from external networks 2 and/or 3, for example, or "off" when the Public Unit 54 is connected to external networks 2 and/or 3 (all exclusive of external wireless transmitters or receivers of the PC1 and/or microchip 90 and/or 501).

An architecture for any computer and/or microchip (or nanochip) can have any number of inner hardware-based access barriers or firewalls 50b arranged in any configuration.

Figure 4 is a similar useful architectural example embodiment to that shown in Figure 2 and 3, but with Private Unit 53 and Public Unit 54 connected in terms of communication of data or code by an inner hardware-based access barrier or firewall 50c example that also includes an output on/off switch and/or microcircuit equivalent 58 on the secure out-only bus or channel 55, in addition to the input on/off switch and/or microcircuit (or nano-circuit) equivalent 57 on the in-only bus or channel 56.

The output switch or microcircuit equivalent 58 is capable of disconnecting the Public Unit 54 from the Private Unit 53 when the Public Unit 54 is being permitted by the master controller 30 (or 31 or 93 or 93') to perform a private operation controlled (completely or in part) by an authorized third party user from the Internet 3, as discussed previously by the applicant relative to Figure 17D and associated textual specification of the '657 Application incorporated above. The user 49 using the master controller 30 (or 31 or 93 or 93') always remains in preemptive control on the Public Unit 54 and can at any time for any reason interrupt or terminate any such third party-controlled operation. The master controller 30 (or 31 or 93 or 93') controls both on/off switches 57 and 58 and

traffic (data and code) on both buses or channels 55 and 56 and the control can be hardwired.

Another example is an equivalent connection, such as a wireless connection, to the in-only bus or channel 56 and out-only bus or channel 55, each with an on/off switch 57 and 58 between the two Units 53 and 54, would require at least one wireless transmitter and at least one receiver in the Private Unit 53, as well as at least one transmitter and at least one receiver in the Public Unit 54, so the Private Unit 53 can send or receive data or code to or from the Public Unit 54 by directly controlling the "on" or "off" state of its transmitter and receiver, controlling that flow of data or code depending, for example on the state of external network 2 or Internet 3 connection of the Public Unit 54 (again, all exclusive of external wireless transmitters or receivers of the PC1 and/or microchip 90 and/or 501).

An architecture for any computer and/or microchip (or nanochip) can have any number of inner hardware-based access barriers or firewalls 50c arranged in any configuration.

Figure 5 shows an architectural example embodiment of a first computer (personal computer 1 and/or microchip 90 and/or 501 or wafer 1500, or 1501, 1502, or 1503) functioning as a Private Unit 53' that is connected to at least a second computer (or to a multitude of computers, including personal computers 1 and/or microchips 90 and/or 501 or 1500, 1501, 1502, or 1503) functioning as a Public Unit or Units 54'. The connection between the private computer 53' and the public computer or computers 54' is made including the same inner hardware-based access barrier or firewall 50c architecture that includes the same buses and channels 55 and 56 with the same on/off switches 57 and 58 as previously described above in the Figure 4 example above and can use the same

hardwire control. Alternatively, inner hardware-based access barriers or firewalls 50a or 50b can be used. In addition, inner hardware-based access barriers or firewalls 50a, 50b, and 50c can be used within the first and/or second computers.

The connection between the first and second computer can be any connection, including a wired network connection like the Ethernet, for example, or a wireless network connection, similar to the examples described above in previous Figures 2-4. In the Ethernet example, either on/off switch 57 or 58 can be functionally replaced like in a wireless connection by control of an output transmitter or an input receiver on either bus or channel 55 or 56; the transmitter or receiver being turned on or off, which of course amounts functionally to mere locating the on/off switches 55 or 56 in the proper position on the bus or channel 55 or 56 to control the appropriate transmitter or receiver, as is true for the examples in previous figures.

Figure 6 shows a useful architectural example embodiment of any computer (a personal computer 1 and/or microchip 90 and/or 501 or wafer 1500, 1501, 1502, or 1503) similar to Figures 23A and 23B of the '657 Application incorporated by reference above, which showed multiple inner firewalls 50 with progressively greater protection. Figure 6 shows an example of an internal array of inner hardware-based access barriers or firewalls 50c, 50b, and 50a (described in previous Figures 2-4 above) used in a specific sequence between a public unit 54 and a first private unit 53, between the first private unit 53 and a more private second unit 53^1, and between the more private second unit 53^1 and a most private third unit 53^2, respectively.

In addition, Figure 6 shows a useful architectural example embodiment of one or more master controllers-only C (31 or 93') located in the most private unit 53^2, with one or more microprocessors or processing units or "cores" S (40 or 94) located in the more

private unit 53^1, in the private unit 53, and in the public unit 54. Each of the microprocessors or processing units or cores S can have at least one secondary controller 32 with which it can be integrated, for example.

The microprocessors S (or processing units or cores) can be located in any of the computer units, but the majority in a many core architecture can be in the public unit to maximize sharing and Internet use. Alternatively, for computers that are designed for more security-oriented applications, a majority of the microprocessors S (or processing units or cores) can be located in the private units; any allocation between the public and private units is possible. Any other hardware, software, or firmware component or components can be located in the same manner as are microprocessors S (or master controllers-only C) described above.

An architecture for any computer and/or microchip or nanochip can have any number of inner hardware-based access barriers or firewalls 50a and/or 50b and/or 50c arranged in any combination or configuration.

As shown in Figure 6, the private non-Internet network 52, which was discussed previously relative to Figure 1, can consist in an example embodiment of more than one network, with each additional non-Internet network 52 being used to connect Private Units 53^2, 53^1, and 53 of one computer and/or microchip to separate non-Internet networks 52^2, 52^1 and 52, respectively, and that are connected to Private Units 53^2, 53^1, and 53, respectively, of other computers and/or microchips. That is, each computer and/or microchip Private Unit 53^2, 53^1, and 53 can have its own separate, non-Internet network 52^2, 52^1, and 52, respectively, and so that any Private Unit can be connected to other computer PC1 and/or microchip 90 (and/or 501) units of the same level of security; any Private Unit can also be subdivided into subunits of the same level of security. This is a

useful embodiment example for making relatively local connections from business or home networks and scales up to large business servers, cloud, or supercomputers applications. The connections can be wired or wireless and local or non-local.

Similarly, a computer PC1 and/or microchip 90 or 501 Public Unit 54 can be subdivided into a number of different levels of security, for example, and each subdivided Public Unit 54 can have a separate, non-Internet connected network 52; and a subdivided Public Unit 54 can be further subdivided with the same level of security. In addition, any hardware component (like a hard drive or Flash memory device (and associated software or firmware), within a private (or public) unit of a given level of security can be connected by a separate non-Internet network 52 to similar components within a private (or public) unit of the same level of security.

Any configuration of access barriers or firewalls 50a and/or 50b and/or 50c can be located between any of the private non-Internet-connected networks 52^2, 52^1, and 52, and the Private Units 53^2, 53^1, and 53, respectively, providing a useful example of increased security control as shown in Figure 6.

Also shown in the example embodiment of Figure 6, each Private Unit 53^2, 53^1, and 53 can have one or more ports (or connections to one or more ports), like for a USB connection to allow for the use of one or more optional removable access and/or encryption or other keys 46, and/or one or more optional removable memory (such as a USB Flash memory thumbdrive) or other device 47, both of which as discussed previously in the text of Figure 1, which example can also have one or more ports for either 46 and/or 47 and/or other device. The Public Unit 54 can also have one or more of any such removable devices, or ports like a USB port to allow for them.

Any data or code or system state, for example, for any Public or Private Unit 54 or

53 can be displayed to the personal user 49 and can be shown in its own distinctive color or shading or border (or any other visual or audible distinctive characteristic, like the use of flashing text). Figure 6 shows an example embodiment of different colors indicated for each of the Units.

For embodiments requiring a higher level of security, it may be preferable to eliminate permanently or temporarily block (by default or by user choice, for example) the non-Internet network 52^2 and all ports or port connections in the most private unit 53^2.

The public unit 54 can be subdivided into an encrypted area (and can include encryption/decryption hardware) and an open, unencrypted area, as can any of the private units 53; in both cases the master central controller 30, 31, 93, or 93' can control the transfer of any or all code or data between an encrypted area and an unencrypted area considering factors such authentication.

The invention example structural and functional embodiments shown in the above described Figures 1-6, as well as the following Figures 7-16 and the associated textual specification of this application all most directly relate to the example structural and functional embodiments of the inner firewall 50 described in Figures 10A-10D, 10J-10Q, 17A-17D, 23A-23E, 24, 25A-25D and 27A-27G, and associated textual specification, of the above '657 Application incorporated by reference.

Figures 7-14 are useful architectural example embodiments of the inner hardware-based access barriers or firewalls 50a, 50b, and 50c.

Figure 7 shows the fundamental security problem caused by the Internet connection to the classic Von Neumann computer hardware architecture that was created in 1945. At that time there were no other computers and therefore no networks of even the simplest kind, so network security was not a consideration in its fundamental design.

Figure 8 shows a useful example embodiment of the applicant's basic architectural solution to the fundamental security problem caused by the Internet, the solution being to protect the central controller of the computer with an inner firewall 50 controlling access by the Internet, as discussed in detail in Figures 10A-10D and 10J-10Q, and associated textual specification of the '657 Application incorporated by reference, as well as earlier in this application. Figure 8 and subsequent figures describe example embodiments of a number of specific forms of an inner hardware-based access barrier or firewall 50, such as access barriers or firewalls 50a and/or 50b and/or 50c as described previously in this application; the number and potential configurations of access barriers or firewalls 50a and/or 50b and/or 50c within any computer, such as computer PC 1 and/or microchip 90 (and/or 501) is without any particular limit.

Figure 9 is a similar embodiment to Figure 8, but also showing a useful architectural example of a central controller integrated with a microprocessor to form a conventional general purpose microprocessor or CPU (like an Intel x86 microprocessor, for example). Figure 8 also shows a computer PC1 and/or microchip 90 and/or 501 with many microprocessors or cores.

Figure 10 is the same embodiment as Figure 9, but also shows a major functional benefit of the applicant's access barrier or firewall 50a, 50b, and 50c invention, which is to enable a function to flush away Internet malware by limiting the memory access of malware to DRAM 66 (dynamic random access memory) in the Public Unit 54, which is a useful example of a volatile memory that can be easily and quickly erased by power interruption. The flushing function of a firewall 50 was discussed earlier in detail in Figures 25A-25D and associated textual specification of the '657 Application incorporated by reference earlier.

Figure 11 is a useful example embodiment similar to Figure 6 and shows that any computer or microchip can be partitioned into many different layers of public units 54 and private units 53 using an architectural configuration of access barriers or firewalls 50a, 50b, and 50c; the number and arrangement of potential configurations is without any particular limit. The partition architecture provided by firewalls 50 was discussed earlier in detail in Figures 23A-23B and associated textual specification of the '657 Application incorporated by reference earlier.

Figure 12 is another useful architectural example embodiment of the layered use of access barriers or firewalls 50, 50c, 50b, and 50c based on a kernel or onion structure; the number of potential configurations is without any particular limit. This structure was discussed in detail relative to firewalls 50 in Figures 23D-23E and associated textual specification of the '657 Application incorporated by reference earlier.

Figure 13 is a useful architectural example embodiment showing the presence of many Figure 12 layered access barriers or firewalls 50a, 50b, and 50c structures on any of the many hardware, software, and/or firmware components of a computer; the number of potential configurations is without any particular limit. The many layered kernels structure was discussed in more detail in Figure 23C and associated textual specification of the '657 Application incorporated by reference earlier.

Figure 14 is a useful architectural example embodiment similar to Figure 13, but also showing the computer PC1 and/or microchip 90 and/or 501 surrounded by a Faraday Cage 300; the number of potential similar configurations is without any particular limit. This use of Faraday Cages 300 was discussed in detail in Figures 27A-27G and associated textual specification of the '657 Application incorporated by reference earlier.

Figure 14 shows a useful example embodiment of a Faraday Cage 300

surrounding completely a computer PC1 and/or microchip 90 and/or 501. The Faraday Cage 300 can be subdivided by an example partition 301 to protect and separate the Private Unit 53 from the Public Unit 54, so that the Private Unit 53 is completely surrounded by Faraday Cage 300^1 and Public Unit 54 is completely surrounded by Faraday Cage 300^2, in the example embodiment shown. Each unit can alternatively have a discrete Faraday Cage 300 of its own, instead of partitioning a larger Faraday Cage 300 and the surrounding of a Unit can be complete or partial. Any number or configuration of Faraday Cages can be used in the manner shown generally in Figure 14, including a separate Faraday Cage for any hardware component of the computer or microchip.

The example embodiments shown in Figures 1-4, 6-11, and 13-16 are a computer of any sort, including a personal computer PC1; or a microchip 90 or 501, including a microprocessor or a system on a chip (SoC) such as a personal computer on a microchip 90; or a combination of both, such as a computer with the architecture shown in Figures 1-4, 6-11, and 13-16, the computer also including one or more microchips also with the architecture shown in Figures 1-4, 6-11, and 13-16.

The Public Unit 54 shown in Figures 1-6, 8-11, and 13-14 can be used in a useful embodiment example to run all or a part of any application (or "apps") downloaded from the Internet or Web, such as the example of any of the many thousands of apps for the Apple iPhone that are downloaded from the Apple Apps Store, or to run applications that are streamed from the Internet or Web. Similarly, all or part of a video or audio file like a movie or music can be downloaded from the Web and played in the Public Unit 54 for viewing and/or listening be the computer user 49.

Some or all personal data pertaining to a user 49 can be kept exclusively on the user's computer PC1 and/or microchip 90 and/or 501 for any cloud application or app to

protect the privacy of the user 49 (or kept non-exclusively as a back-up), unlike conventional cloud apps, where the data of a personal user 49 is kept in the cloud and potentially intentionally shared or carelessly compromised without authorization by or knowledge of the personal user 49. In effect, the Public Unit 54 can be a safe and private local cloud, with personal files retained there or in the Private Unit 53. All or part of an app can also potentially be downloaded or streamed to one or more Private Units, including 53^2, 53^1, and 53.

Privacy in conventional clouds can also be significantly enhanced using the inner hardware-based access barriers or firewalls 50a and/or 50b and/or 50c described in this application, since each individual or corporate user of the cloud can be assured that their data is safe because it can be physically separated and segregated by hardware, instead of by software alone, as is the case currently.

Similarly, the example embodiment of Figure 6 shows a computer and/or microchip Public Unit 54 and Private Units 53, 53^1, and 53^2, each with a separate Faraday Cage. 300^4, 300^3, 300^2, and 300^1, respectively, that are create using partitions 301^c, 301^b, and 301^a, respectively. Any Public Unit 54 or Private Unit 53 can be protected by its own Faraday Cage 300. The Faraday Cage 300 can completely or partially surround the any Unit in two or three dimensions.

Figures 8-11 and 13-14 also show example embodiments of a secure control bus (or wire or channel) 48 that connects the master controlling device 30 (or 31) or master control unit 93 (or 93') or central controller (as shown) with the components of the computer PC1 and/or microchip 90 and/or 501, including those in the Public Unit 54. The secure control bus 48 provides hardwired control of the Public Unit 54 by the central controller in the Private Unit 53. The secure control bus 48 can be isolated from any input

from the Internet 3 and/or an intervening other network 2 and/or from any input from any or all parts of the Public Unit 54. The secure control bus 48 can provide and ensure direct preemptive control by the central controller over any or all the components of the computer, including the Public Unit 54 components. The secure control bus 48 can, partially or completely, coincide or be integrated with the bus 55, for example. The secure control bus 48 is configured in a manner such that it cannot be affected, interfered with, altered, read or written to, or superseded by any part of the Public Unit 54 or any input from the Internet 3 or network 2, for example. A wireless connection can also provide the function of the secure control bus 48 a manner similar to that describing wireless connections above in Figures 2-6 describing buses 55 and 56.

The secure control bus 48 can also provide connection for the central controller to control a conventional firewall or for example access barrier or firewall 50c located on the periphery of the computer or microchip to control the connection of the computer PC1 and/or microchip 90 and/or 501 to the Internet 3 and/or intervening other network 2.

The secure control bus 48 can also be used by the master central controller 30, 31, 93, or 93' to control one or more secondary controllers 32 located on the bus 49 or anywhere in the computer PC1 and/or microchip 90 and/or 501, including in the Public Unit 54 that are used, for example, to control microprocessors or processing units or cores S (40 or 94) located in the Public Unit 54. The one or more secondary controllers 32 can be independent or integrated with the microprocessors or processing units or cores S (40 or 94) shown in Figure 9 and 11 above, for example; such integrated microprocessors can be specially designed or general purpose microprocessors like an Intel x86 microprocessor, for example.

In accordance with the present disclosure, a method of protecting a computer is

disclosed in Fig. 15. The computer includes a master controlling device that is configured using hardware and firmware; at least two microprocessors; a protected portion of the computer; an unprotected portion of the computer; and an inner hardware-based access barrier or firewall that is located between the protected portion of the computer and the unprotected portion of the computer, the protected portion including at least the master controlling device and at least one of the microprocessors, and the unprotected portion including at least one of the microprocessors, the at least one microprocessor of the unprotected portion being separate from and located outside of the inner hardware-based access barrier or firewall. As shown in Fig. 15, the method includes allowing a user of the computer to control the microprocessors (150); connecting the protected portion of the computer through a first connection to at least a first network of computers (152); connecting the unprotected portion of the computer through a second connection to a second network of computers including the Internet (154); denying access by the hardware-based access barrier or firewall to the protected portion of the computer by the second network when the personal computer is connected to the second network (156); and permitting access by another computer in the second network to the one or more of the processing units included in the unprotected portion of the microchip for an operation with the another computer in the second network when the personal computer is connected to the second network (158).

In accordance with the present disclosure, a method of protecting a computer disclosed in Fig. 16. The computer includes a master controlling device that is configured using hardware and firmware; at least two microprocessors; a protected portion of the computer; an unprotected portion of the computer; and an inner hardware-based access barrier or firewall that is located between the protected portion of the computer and the

unprotected portion of the computer, the protected portion including at least the master controlling device and at least one of the microprocessors, and the unprotected portion including at least one of the microprocessors, the at least one microprocessor of the unprotected portion being separate from and located outside of the inner hardware-based access barrier or firewall. As shown in Fig. 16, the method includes connecting the protected portion of the computer through at least a first connection to at least a first network of computers (160); connecting the unprotected portion of the computer through a second connection to a second network of computers including the Internet (162); controlling the computer from the protected portion through the first network (164); and performing operations in the unprotected portion using the second network (166).

Any one or more features or components of Figures 1-16 of this application can be usefully combined with one or more features or components of Figures 1-31 of the above '657 U.S. Application or Figures 1-27 of the above '769 U.S. Application. Each of the above '657 and '769 Applications and their associated U.S. publications are expressly incorporated by reference in its entirety for completeness of disclosure of the applicant's combination of one or more features or components of either of those above two prior applications of this applicant with one or more features or components of this application. All such useful possible combinations are hereby expressly intended by this applicant.

Furthermore, any one or more features or components of Figures 1-16 of this application can be usefully combined with one or more features or components of the figures of the above '049 and '553 U.S. Applications, as well as in the above '428, '250, '141, '449, '906, '275, '020, '854, '529, '756, and '233 U.S. Patents. Each of the above '049 and '553 Applications and their associated U.S. publications, as well as the above '428, '250, '141, '449, '906, '275, '020, '854, '529, '756, and '233 U.S. Patents are

expressly incorporated by reference in its entirety for completeness of disclosure of the applicant's combination of one or more features or components of either of those above two prior applications of this applicant with one or more features or components of this application. All such useful possible combinations are hereby expressly intended by this applicant.

In addition, one or more features or components of any one of Figures 1-16 or associated textual specification of this application can be usefully combined with one or more features or components of any one or more other of Figures 1-16 or associated textual specification of this application. And any such combination derived from the figures or associated text of this application can also be combined with any feature or component of the figures or associated text of any of the above incorporated by reference U.S. Applications '657, '769, '049, and '553, as well as U.S. Patents Numbers '428, '250, '141, '449, '906, '275, '020, '854, '529, '756, and '233.

CLAIMS:

1. A personal computer, comprising:

a microchip including

a microprocessor, the microprocessor including

a master control unit that is configured using hardware and firmware, and

at least two processing units;

the master control unit of the microprocessor being further configured to allow a user of the personal computer to control the processing units of the microprocessor;

an inner hardware-based access barrier or firewall that is located between a protected portion of the microchip and an unprotected portion of the microchip;

said protected portion of the microchip being configured for at least a first connection to at least a first network of computers and including

at least said master control unit of the microprocessor and

at least one of the processing units of the microprocessor,

said unprotected portion of the microchip being configured for a second connection to a second network of computers including the Internet and including one or more of the processing units of the microprocessor, said one or more unprotected processing units being separate from and located outside of said inner hardware-based access barrier or firewall;

said inner hardware-based access barrier or firewall denying access to said protected portion of the microchip by a network including the Internet when the

personal computer is connected to the network including the Internet; and

said inner hardware-based access barrier or firewall permitting access by another computer in the network including the Internet to said one or more of the processing units included in the unprotected portion of the microchip for an operation with said another computer in the network including the Internet when the personal computer is connected to the network including the Internet.

2. A computer, comprising:

a master controlling device that is configured using hardware and firmware,

at least two microprocessors; and

the master controlling device of the computer being further configured to allow a user of the computer to control the microprocessors;

an inner hardware-based access barrier or firewall that is located between a protected portion of the computer and an unprotected portion of the computer;

said protected portion of the computer being configured for at least a first connection to at least a first network of computers and including

at least said master controlling device and

at least one of the microprocessors,

said unprotected portion of the computer being configured for a second connection to a second network of computers including the Internet and including one or more of the microprocessors, said one or more unprotected microprocessors being separate from and located outside of said inner hardware-based access barrier or firewall;

said hardware-based access barrier or firewall denying access to said protected portion of the computer by a network including the Internet when the computer

is connected to the network including the Internet; and

said hardware-based access barrier or firewall permitting access by another computer in the network including the Internet to said one or more of the microprocessors included in the unprotected portion of the computer for an operation with said another computer in the network including the Internet when the computer is connected to the network including the Internet.

3. A microchip, comprising:

a microprocessor, the microprocessor including

a master control unit that is configured using hardware and firmware, and

at least two processing units;

the master control unit of the microprocessor being further configured to allow a user of the microchip to control the processing units of the microprocessor;

an inner hardware-based access barrier or firewall that is located between a protected portion of the microchip and an unprotected portion of the microchip;

said protected portion of the microchip configured for at least a first connection to at least a first network of computers and including

at least said master control unit of the microprocessor and

at least one of the processing units of the microprocessor,

said unprotected portion of the microchip configured for a second connection to a second network of computers including the Internet and including one or more of the processing units of the microprocessor, said one or more unprotected processing units being separate from and located outside of said inner hardware-based

access barrier or firewall;

said hardware-based access barrier or firewall denying access to said protected portion of the microchip by a network including the Internet when the computer is connected to the network including the Internet; and

said hardware-based access barrier or firewall permitting access by another computer in the network including the Internet to said one or more of the processing units included in the unprotected portion of the microchip for an operation with said another computer in the network including the Internet when the microchip is connected to the network including the Internet.

4. The computer of claim 1, wherein said first network excludes the Internet.

5. The computer of claim 2, wherein said first network excludes the Internet.

6. The microchip of claim 3, wherein said first network excludes the Internet.

7. The computer of claim 4, wherein the protected portion and the unprotected portion are connected by an out-only bus or channel that transmits data or code that is output from the protected portion to be input to the unprotected portion.

8. The computer of claim 5, wherein the protected portion and the unprotected portion are connected by an out-only bus or channel that transmits data or code that is output from the protected portion to be input to the unprotected portion.

9. The microchip of claim 6, wherein the protected portion and the unprotected portion are connected by an out-only bus or channel that transmits data or code that is output from the protected portion to be input to the unprotected portion.

10. The computer of claim 7, wherein the protected portion and the unprotected portion also are connected by an in-only bus or channel that includes a hardware input on/off switch or equivalent bus signal interruption mechanism or an equivalently functioning circuit on a microchip or nanochip.

11. The computer of claim 8, wherein the protected portion and the unprotected portion also are connected by an in-only bus or channel that includes a hardware input on/off switch or equivalent bus signal interruption mechanism or an equivalently functioning circuit on a microchip or nanochip.

12. The microchip of claim 9, wherein the protected portion and the unprotected portion also are connected by an in-only bus or channel that includes a hardware input on/off switch or equivalent bus signal interruption mechanism or an equivalently functioning circuit on a microchip or nanochip.

13. The computer of claim 10, wherein the protected portion and the unprotected portion are connected by an out-only bus or channel that also includes a hardware input on/off switch or equivalent bus signal interruption mechanism or an equivalently functioning circuit on a microchip or nanochip.

14. The computer of claim 11, wherein the protected portion and the unprotected portion are connected by an out-only bus or channel that also includes a hardware input on/off switch or equivalent bus signal interruption mechanism or an equivalently functioning circuit on a microchip or nanochip.

15. The microchip of claim 12, wherein the protected portion and the unprotected portion are connected by an out-only bus or channel that also includes a hardware input on/off switch or equivalent bus signal interruption mechanism or an equivalently functioning circuit on a microchip or nanochip.

16. The computer of claim 4, wherein an innermost part of the protected portion is connected to an intermediate part of the protected portion by an out-only bus or channel that transmits data or code that is output from the protected portion to be input to the unprotected portion;

the intermediate part of the protected portion is connected to an outermost part of the protected portion by an out-only bus or channel that transmits data or code that is output from the protected portion to be input to the unprotected portion, and also by an in-only bus or channel that includes a hardware input on/off switch or equivalent bus signal interruption mechanism or an equivalently functioning circuit on a microchip or nanochip; and

the outermost part of the protected portion is connected to the unprotected portion by an out-only bus or channel that transmits data or code that is output from the protected portion to be input to the unprotected portion, and by an in-only bus or channel that includes a hardware input on/off switch or equivalent bus signal interruption mechanism

or an equivalently functioning circuit on a microchip or nanochip, and also by an out-only bus or channel that also includes a hardware input on/off switch or equivalent bus signal interruption mechanism or an equivalently functioning circuit on a microchip or nanochip.

17. The computer of claim 5, wherein an innermost part of the protected portion is connected to an intermediate part of the protected portion by an out-only bus or channel that transmits data or code that is output from the protected portion to be input to the unprotected portion;

the intermediate part of the protected portion is connected to an outermost part of the protected portion by an out-only bus or channel that transmits data or code that is output from the protected portion to be input to the unprotected portion, and also by an in-only bus or channel that includes a hardware input on/off switch or equivalent bus signal interruption mechanism or an equivalently functioning circuit on a microchip or nanochip; and

the outermost part of the protected portion is connected to the unprotected portion by an out-only bus or channel that transmits data or code that is output from the protected portion to be input to the unprotected portion, and by an in-only bus or channel that includes a hardware input on/off switch or equivalent bus signal interruption mechanism or an equivalently functioning circuit on a microchip or nanochip, and also by an out-only bus or channel that also includes a hardware input on/off switch or equivalent bus signal interruption mechanism or an equivalently functioning circuit on a microchip or nanochip.

18. The microchip of claim 6, wherein an innermost part of the protected portion is connected to an intermediate part of the protected portion by an out-only bus or channel

that transmits data or code that is output from the protected portion to be input to the unprotected portion;

the intermediate part of the protected portion is connected to an outermost part of the protected portion by an out-only bus or channel that transmits data or code that is output from the protected portion to be input to the unprotected portion, and also by an in-only bus or channel that includes a hardware input on/off switch or equivalent bus signal interruption mechanism or an equivalently functioning circuit on a microchip or nanochip; and

the outermost part of the protected portion is connected to the unprotected portion by an out-only bus or channel that transmits data or code that is output from the protected portion to be input to the unprotected portion, and by an in-only bus or channel that includes a hardware input on/off switch or equivalent bus signal interruption mechanism or an equivalently functioning circuit on a microchip or nanochip, and also by an out-only bus or channel that also includes a hardware input on/off switch or equivalent bus signal interruption mechanism or an equivalently functioning circuit on a microchip or nanochip.

19. The computer of claim 16, wherein at least the intermediate and outermost parts of the protected portion is each configured for a separate connection to a separate network of computers that excludes the Internet.

20. The computer of claim 17, wherein at least the intermediate and outermost parts of the protected portion is each configured for a separate connection to a separate network of computers that excludes the Internet.

21. The microchip of claim 18, wherein at least the intermediate and outermost parts of the protected portion is each configured for a separate connection to a separate network of computers that excludes the Internet.

22. The computer of claim 19, wherein the computer is fully protected by a Faraday Cage from an external electromagnetic pulse.

23. The computer of claim 20, wherein the computer is fully protected by a Faraday Cage from an external electromagnetic pulse.

24. The computer of claim 21, wherein the computer is fully protected by a Faraday Cage from an external electromagnetic pulse.

25. A method of protecting a personal computer having a microchip including a microprocessor, the microprocessor including a master control unit that is configured using hardware and firmware and includes at least two processing units; an inner hardware-based access barrier or firewall that is located between a protected portion of the microchip and an unprotected portion of the microchip, the protected portion including at least said master control unit of the microprocessor and at least one of the processing units of the microprocessor, and the unprotected portion including one or more unprotected processing units that are separate from and located outside of said inner hardware-based access barrier or firewall, comprising:

allowing a user of the personal computer to control the processing units of the microprocessor;

connecting said protected portion of the microchip through at least a first connection to at least a first network of computers;

connecting said unprotected portion of the microchip through a second connection to a second network of computers including the Internet;

denying access by the hardware-based access barrier or firewall to said protected portion of the microchip by the second network when the personal computer is connected to the second network; and

permitting access by another computer in the second network to said one or more of the processing units included in the unprotected portion of the microchip for an operation with said another computer in the second network when the personal computer is connected to the second network.

26. A method of protecting a computer having a master controlling device that is configured using hardware and firmware; at least two microprocessors; a protected portion of the computer; an unprotected portion of the computer; and an inner hardware-based access barrier or firewall that is located between the protected portion of the computer and the unprotected portion of the computer, the protected portion including at least said master controlling device and at least one of the microprocessors, and the unprotected portion including at least one of the microprocessors, said at least one microprocessor of the unprotected portion being separate from and located outside of said inner hardware-based access barrier or firewall, comprising:

allowing a user of the computer to control the microprocessors;

connecting said protected portion of the computer through at least a first connection to at least a first network of computers;

connecting said unprotected portion of the computer through a second connection to a second network of computers including the Internet;

denying access by the hardware-based access barrier or firewall to said protected portion of the computer by the second network when the personal computer is connected to the second network; and

permitting access by another computer in the second network to said one or more of the processing units included in the unprotected portion of the microchip for an operation with said another computer in the second network when the personal computer is connected to the second network.

27. A method of protecting a computer having a master controlling device that is configured using hardware and firmware; at least two microprocessors; a protected portion of the computer; an unprotected portion of the computer; and an inner hardware-based access barrier or firewall that is located between the protected portion of the computer and the unprotected portion of the computer, the protected portion including at least said master controlling device and at least one of the microprocessors, and the unprotected portion including at least one of the microprocessors, said at least one microprocessor of the unprotected portion being separate from and located outside of said inner hardware-based access barrier or firewall, comprising:

connecting said protected portion of the computer through at least a first connection to at least a first network of computers;

connecting said unprotected portion of the computer through a second connection to a second network of computers including the Internet;

controlling the computer from the protected portion through the first network; and

performing operations in the unprotected portion using the second network.

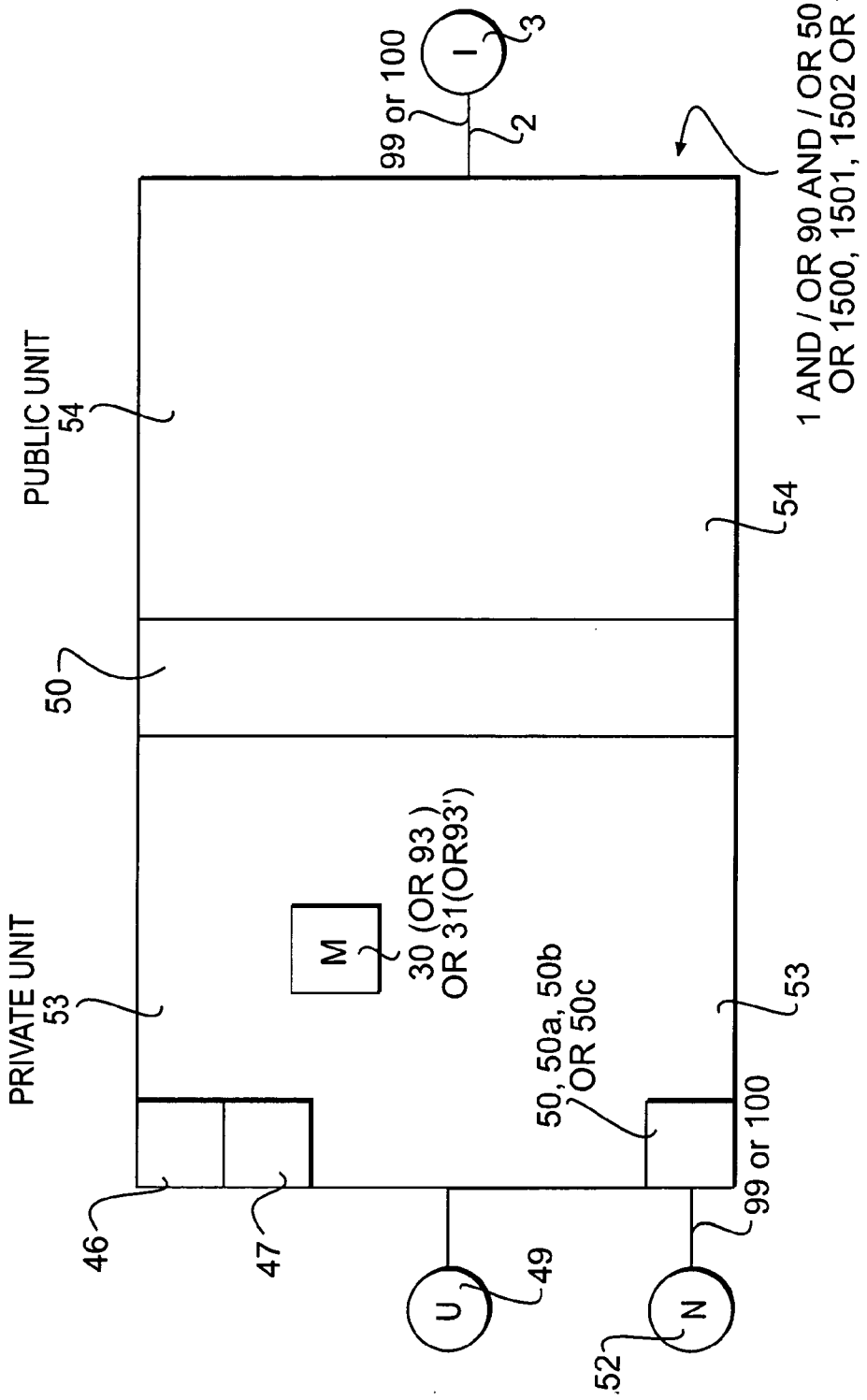
PUBLIC UNIT
54
50
PRIVATE UNIT
53
M
30 (OR 93)
OR 31(OR93')
50, 50a, 50b
OR 50c
99 or 100
I
3
2
1 AND / OR 90 AND / OR 501 AND/
OR 1500, 1501, 1502 OR 1503
54
53
99 or 100
46
47
U
49
N
52

FIG. 1

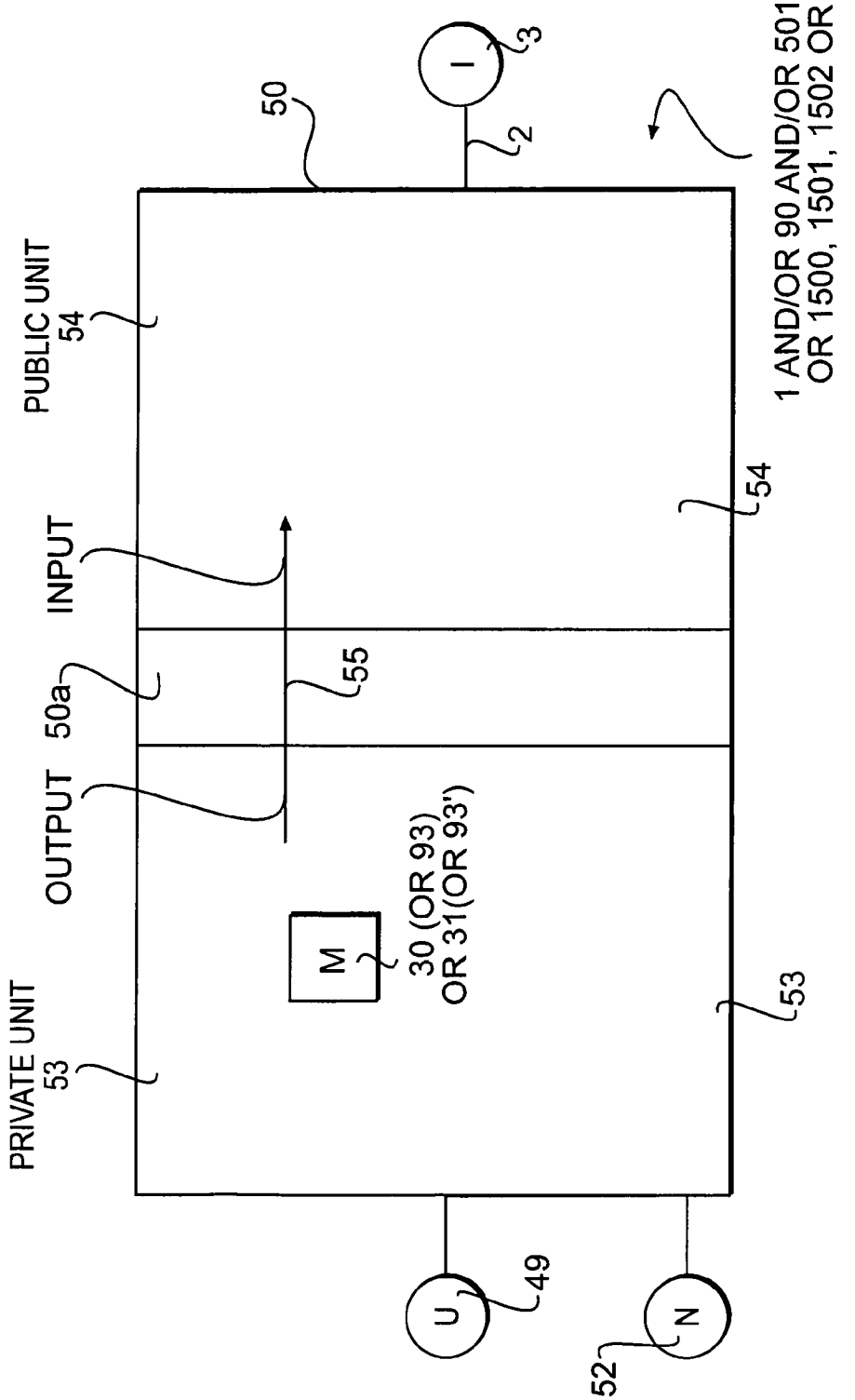
1 AND/OR 90 AND/OR 501 AND/
OR 1500, 1501, 1502 OR 1503
50
I
3
2
PUBLIC UNIT
54
INPUT
54
50a
55
OUTPUT
30 (OR 93)
OR 31(OR 93')
M
PRIVATE UNIT
53
53
U
49
N
52

FIG. 2

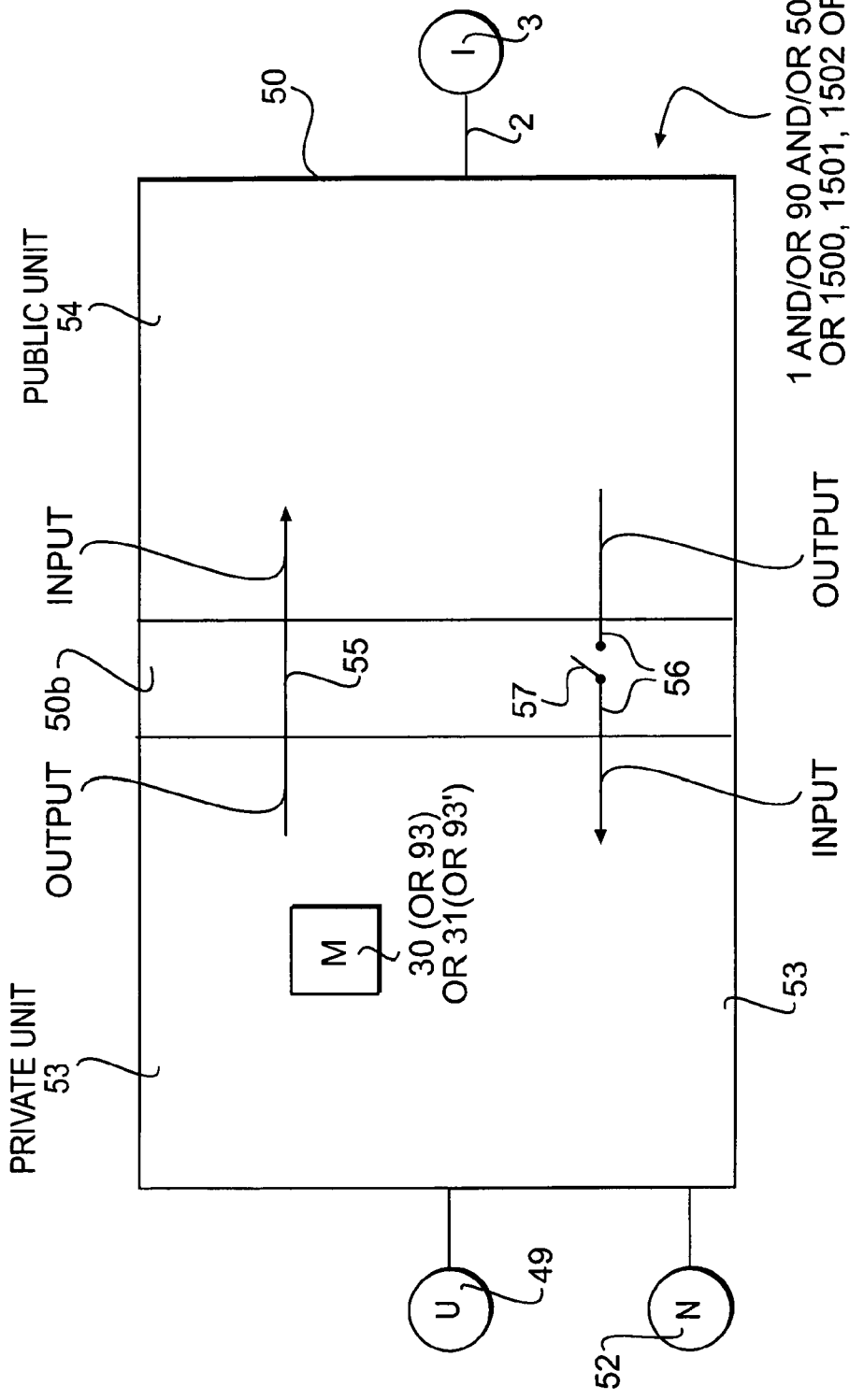
1 AND/OR 90 AND/OR 505 AND/
OR 1500, 1501, 1502 OR 1503
I
3
2
50
PUBLIC UNIT
54
INPUT
OUTPUT
50b
55
57
56
OUTPUT
INPUT
M
30 (OR 93)
OR 31(OR 93')
PRIVATE UNIT
53
53
U
49
N
52

FIG. 3

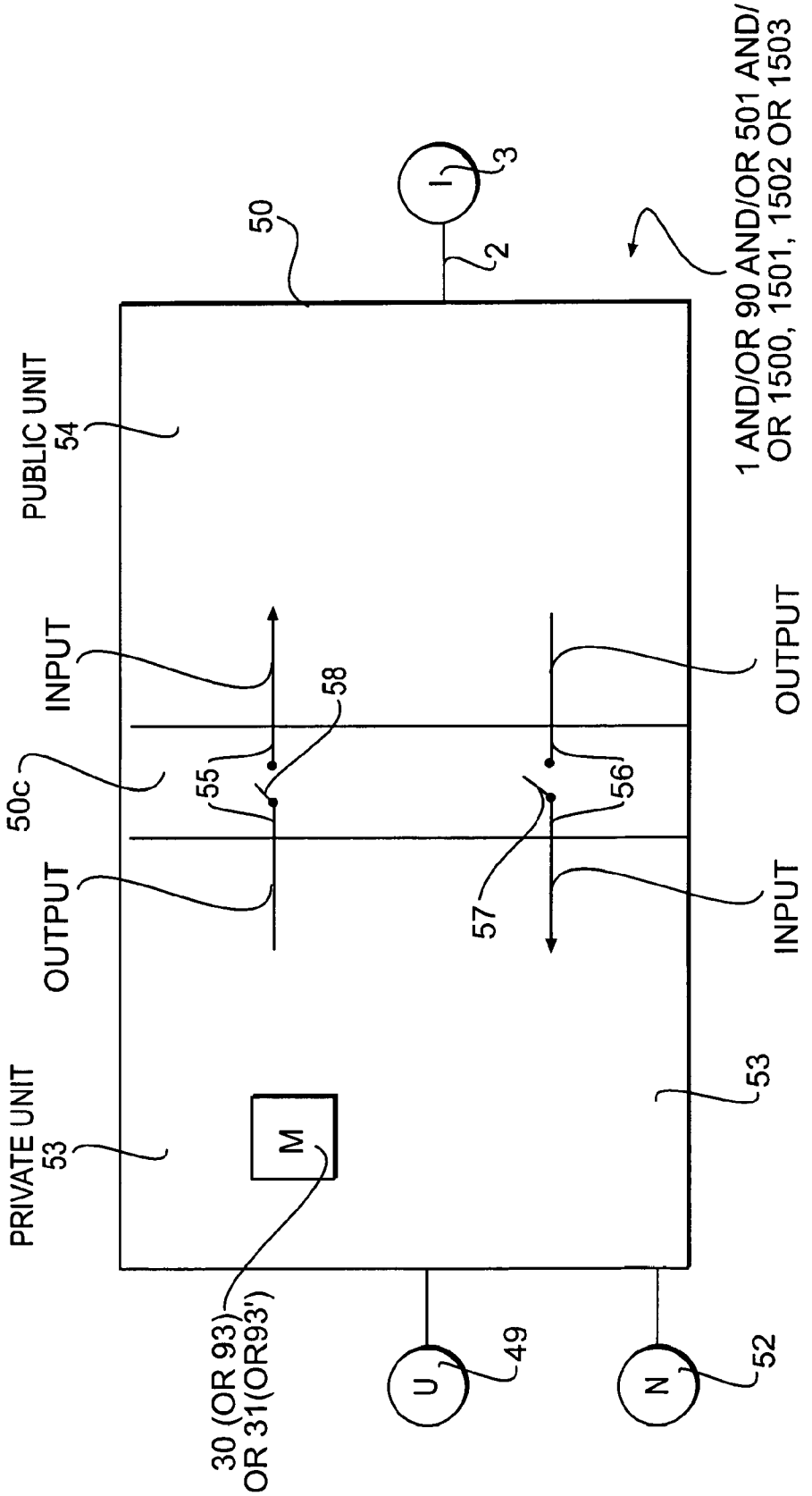
1 AND/OR 90 AND/OR 501 AND/
OR 1500, 1501, 1502 OR 1503
50
I
3
2
PUBLIC UNIT
54
INPUT
OUTPUT
58
55
50c
56
57
OUTPUT
INPUT
PRIVATE UNIT
53
M
53
30 (OR 93)
OR 31(OR93')
U
49
N
52

FIG. 4

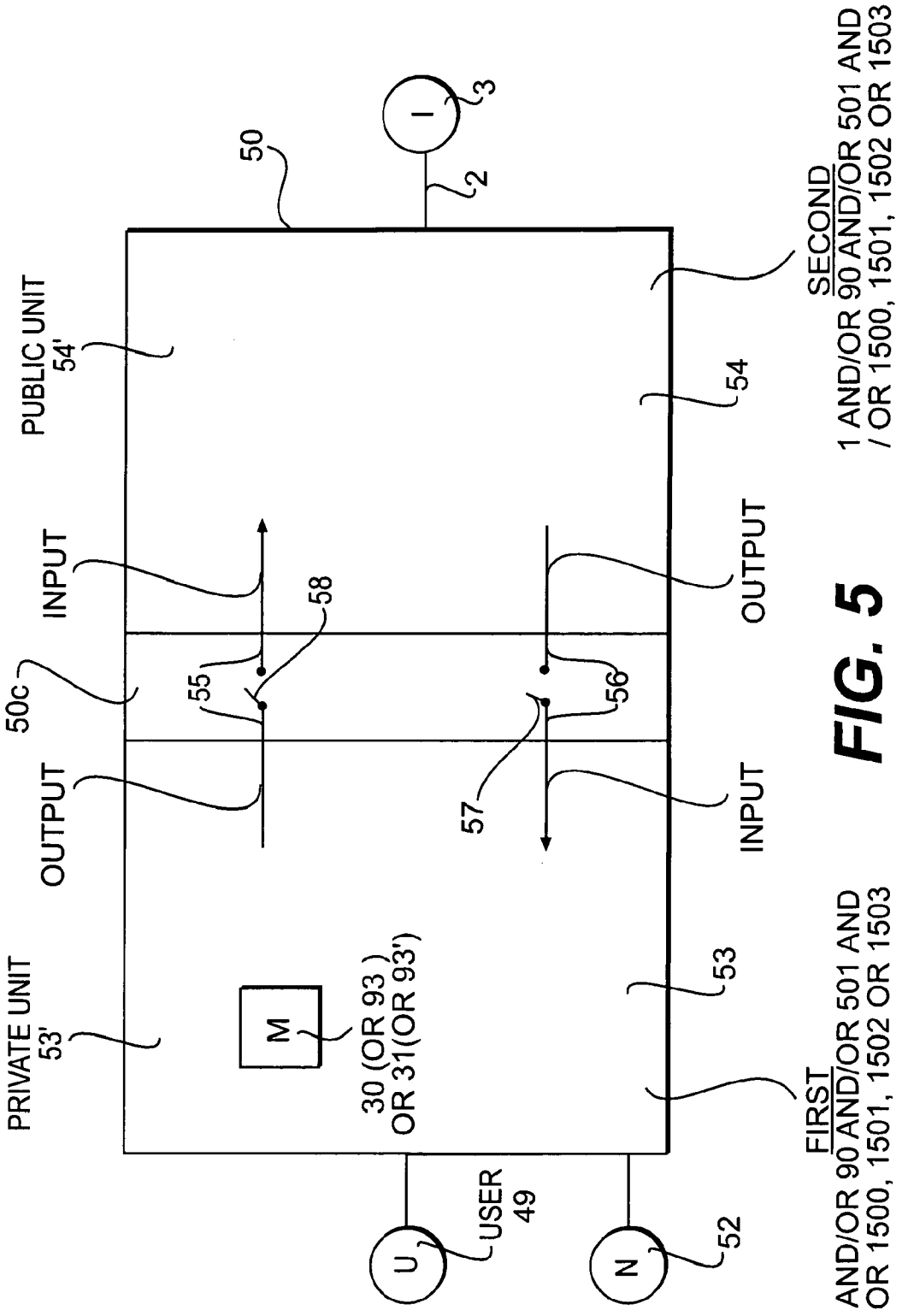
50
I
3
2
PUBLIC UNIT
54'
INPUT
58
55
50c
OUTPUT
PRIVATE UNIT
53'
M
30 (OR 93)
OR 31(OR 93')
USER
49
U
N
52
53
FIRST
1 AND/OR 90 AND/OR 501 AND
/ OR 1500, 1501, 1502 OR 1503
57
INPUT
56
OUTPUT
54
SECOND
1 AND/OR 90 AND/OR 501 AND
/ OR 1500, 1501, 1502 OR 1503

FIG. 5

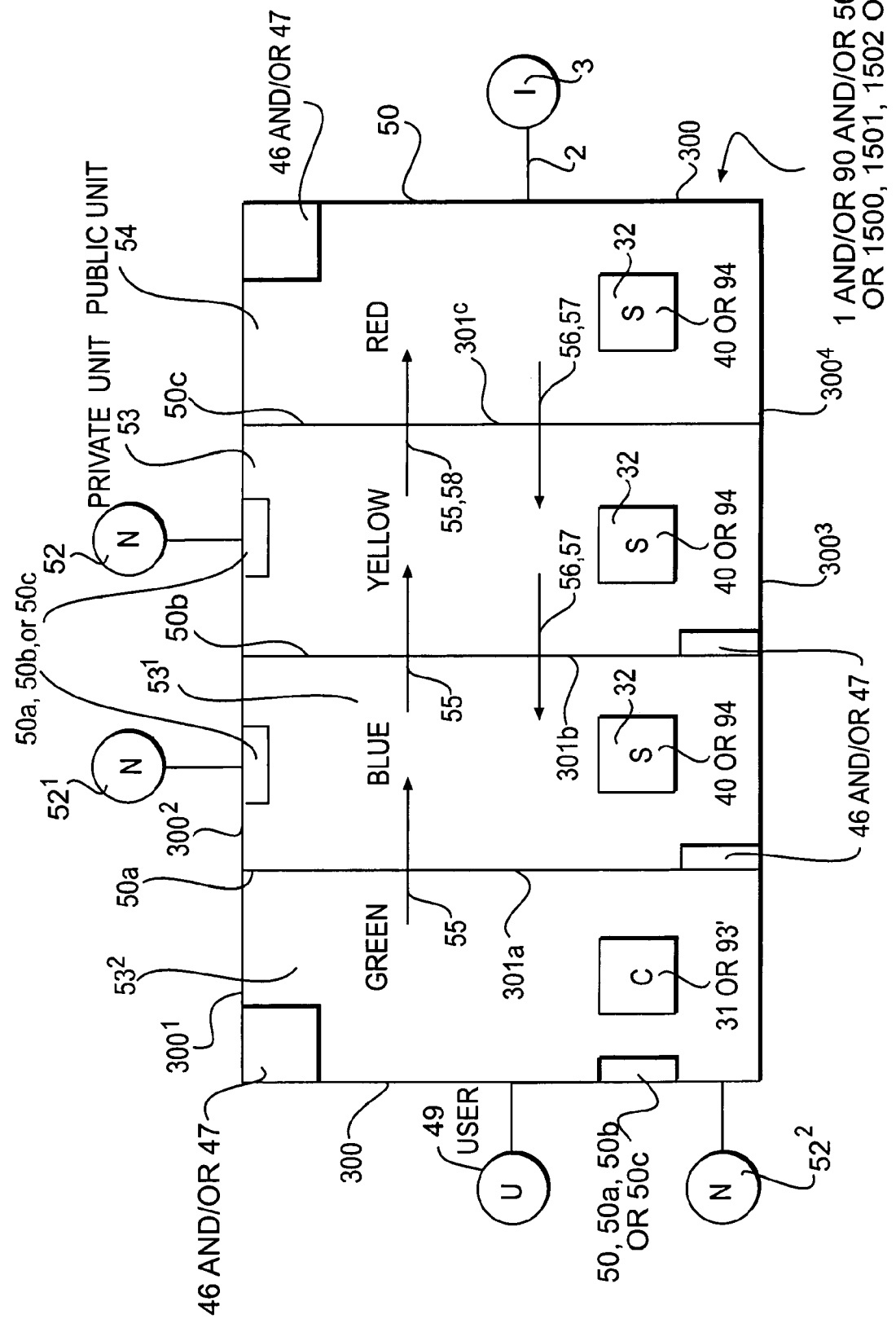
46 AND/OR 47
50
3
2
300
1 AND/OR 90 AND/OR 501 AND/
OR 1500, 1501, 1502 OR 1503
PUBLIC UNIT
54
PRIVATE UNIT
53
52
50a, 50b, or 50c
52^1
53^1
53^2
50a
50b
50c
300^1
300^2
300^3
300^4
RED
YELLOW
BLUE
GREEN
55
55,58
56,57
301a
301b
301c
S
C
32
40 OR 94
31 OR 93'
46 AND/OR 47
49
USER
50, 50a, 50b
OR 50c
52^2

FIG. 6

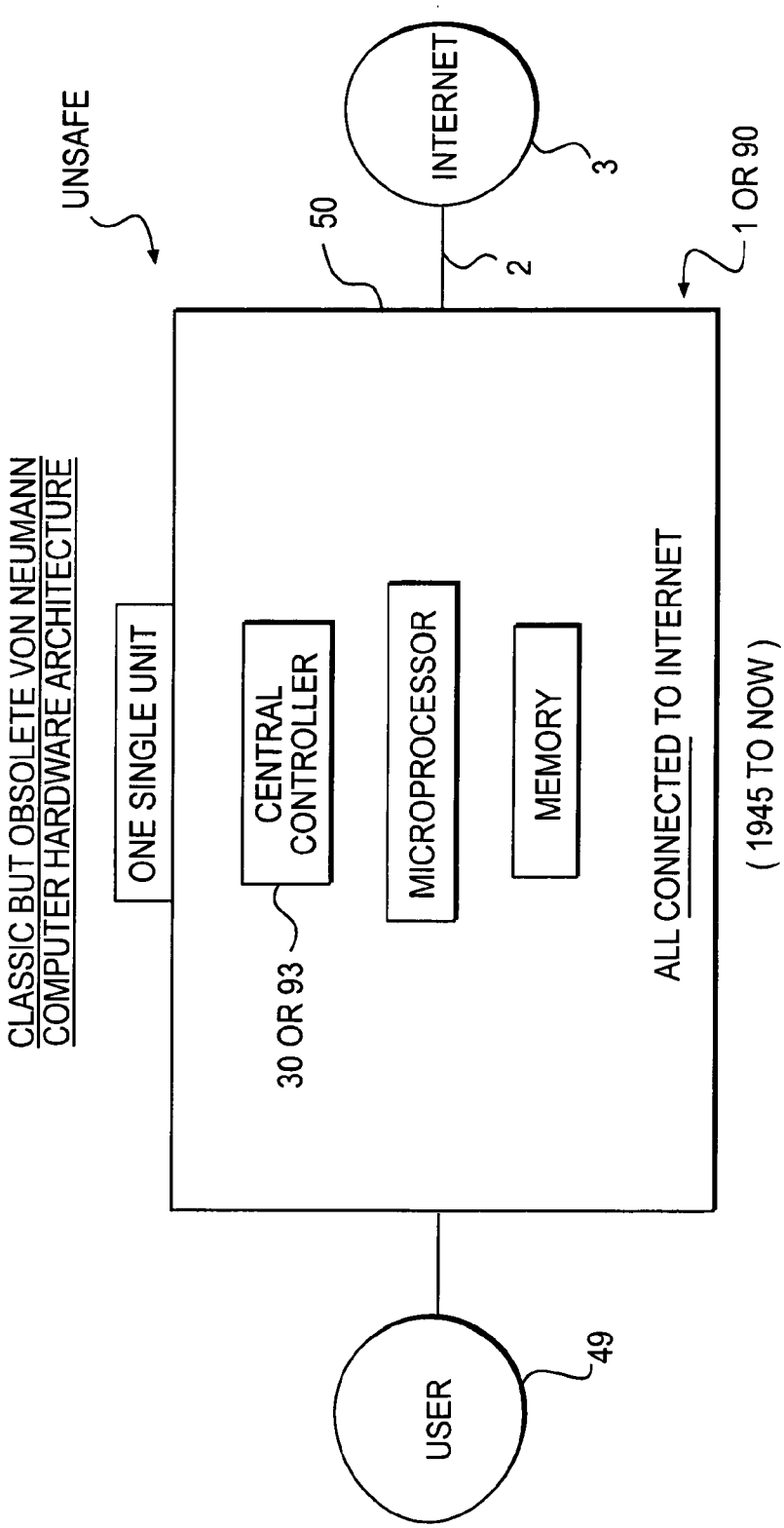
CLASSIC BUT OBSOLETE VON NEUMANN
COMPUTER HARDWARE ARCHITECTURE
ONE SINGLE UNIT
CENTRAL CONTROLLER
30 OR 93
MICROPROCESSOR
MEMORY
ALL CONNECTED TO INTERNET
(1945 TO NOW)
UNSAFE
50
INTERNET
3
2
1 OR 90
USER
49
THE PROBLEM: INTERNET MALWARE HAS POTENTIAL ACCESS
TO ENTIRE COMPUTER TO CONTROL ANY PART OR ALL OF IT

FIG. 7

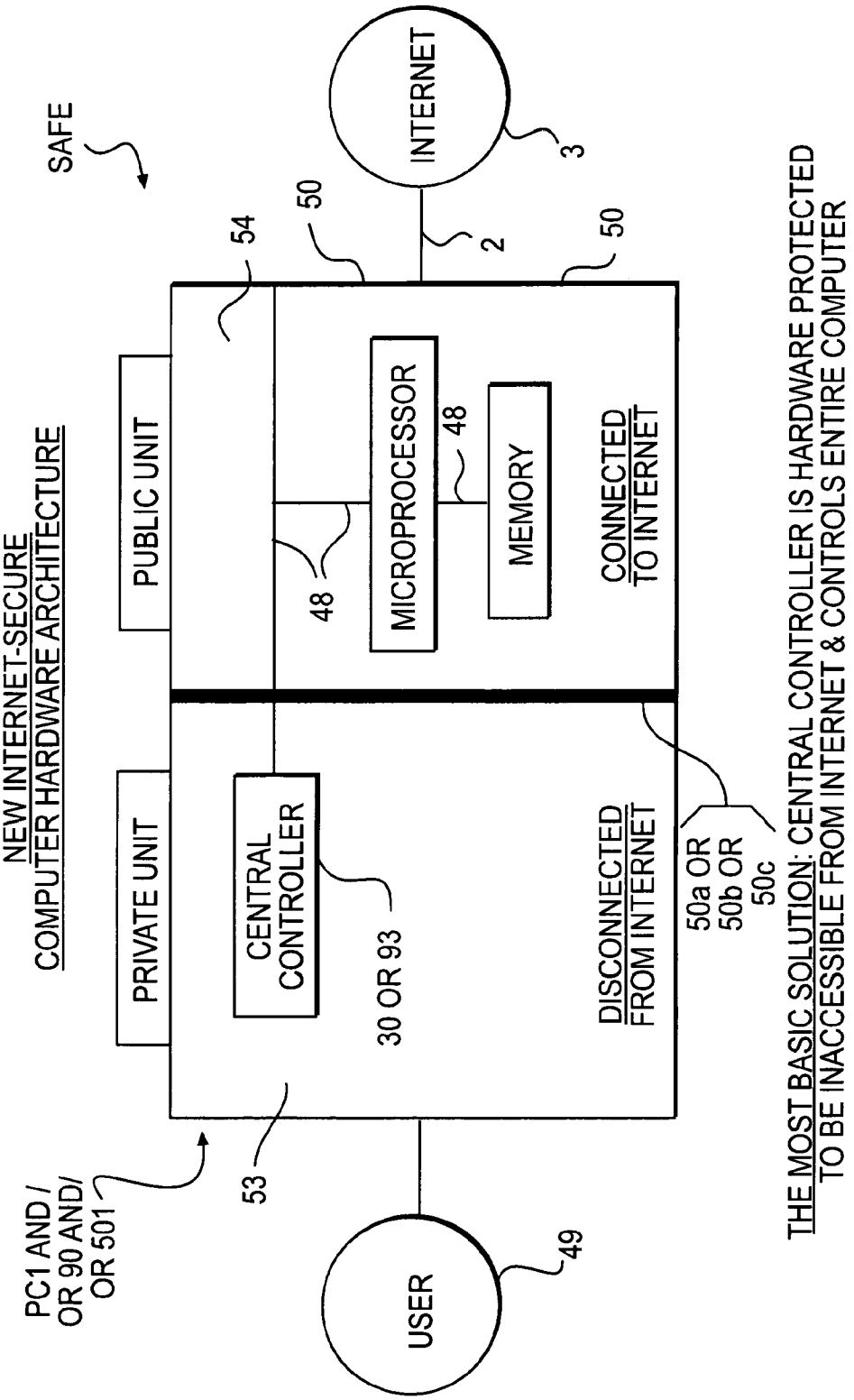
SAFE
INTERNET
3
2
50
50
54
PUBLIC UNIT
MICROPROCESSOR
48
MEMORY
48
CONNECTED TO INTERNET
NEW INTERNET-SECURE COMPUTER HARDWARE ARCHITECTURE
PRIVATE UNIT
CENTRAL CONTROLLER
30 OR 93
DISCONNECTED FROM INTERNET
50a OR 50b OR 50c
THE MOST BASIC SOLUTION: CENTRAL CONTROLLER IS HARDWARE PROTECTED TO BE INACCESSIBLE FROM INTERNET & CONTROLS ENTIRE COMPUTER
PC1 AND / OR 90 AND/ OR 501
53
USER
49

FIG. 8

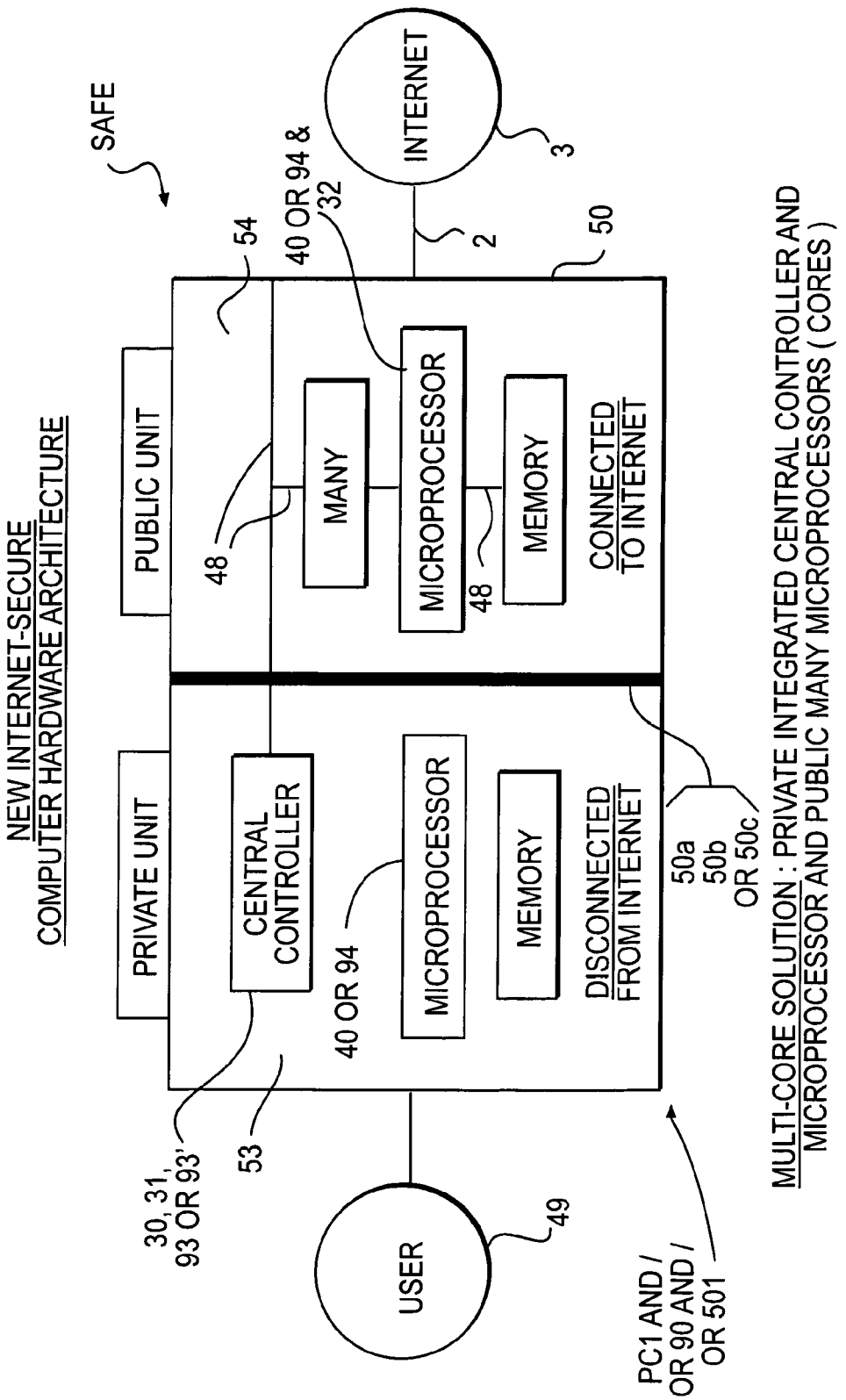
NEW INTERNET-SECURE
COMPUTER HARDWARE ARCHITECTURE
SAFE
INTERNET
3
2
54
40 OR 94 &
32
50
PUBLIC UNIT
48
MANY
MICROPROCESSOR
48
MEMORY
CONNECTED
TO INTERNET
PRIVATE UNIT
CENTRAL
CONTROLLER
40 OR 94
MICROPROCESSOR
MEMORY
DISCONNECTED
FROM INTERNET
50a
50b
OR 50c
30, 31,
93 OR 93'
53
USER
49
PC1 AND /
OR 90 AND /
OR 501
MULTI-CORE SOLUTION : PRIVATE INTEGRATED CENTRAL CONTROLLER AND
MICROPROCESSOR AND PUBLIC MANY MICROPROCESSORS (CORES)

FIG. 9

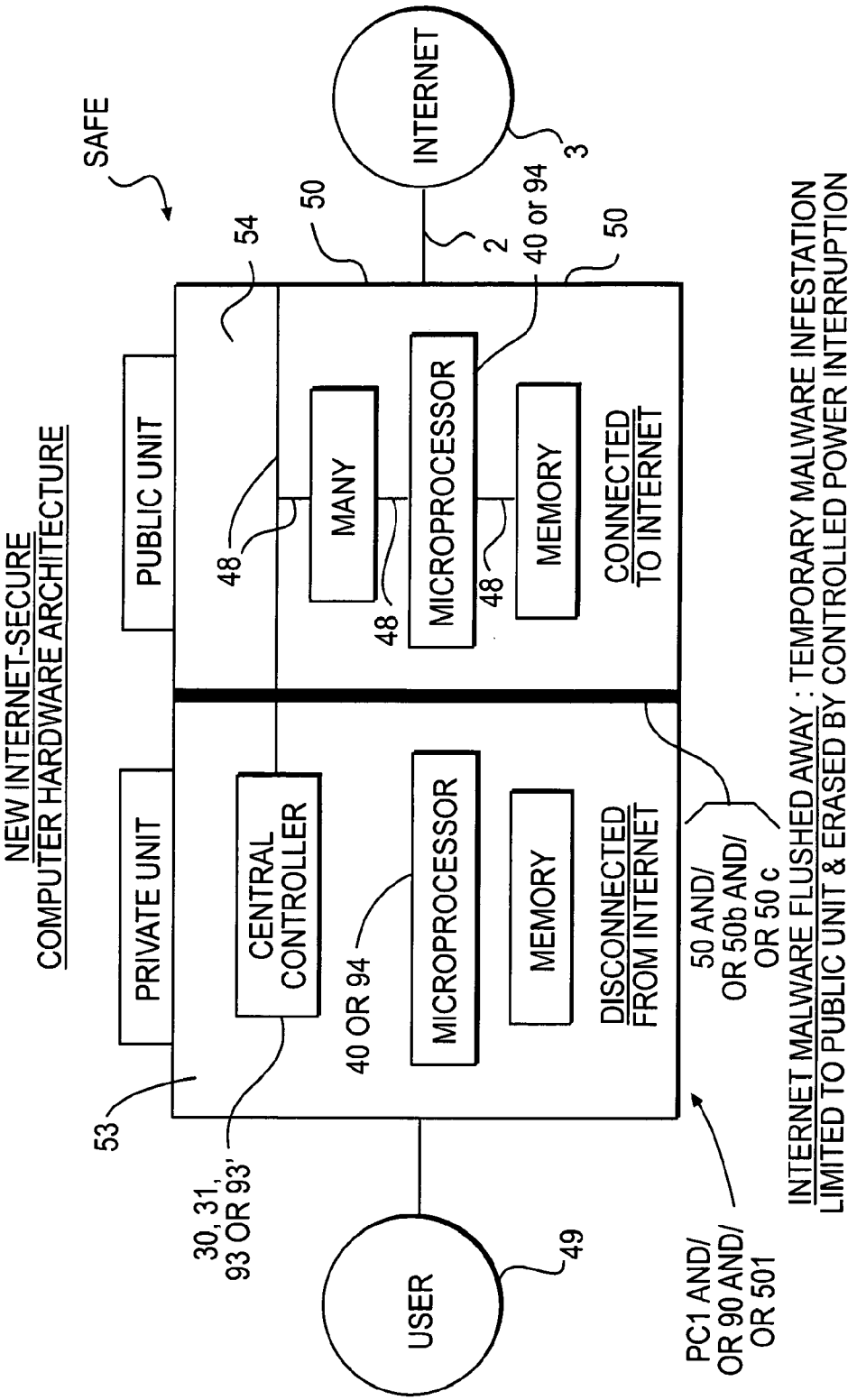
NEW INTERNET-SECURE
COMPUTER HARDWARE ARCHITECTURE
SAFE
INTERNET
3
2
40 or 94
50
54
PUBLIC UNIT
PRIVATE UNIT
MANY
MICROPROCESSOR
MEMORY
CONNECTED
TO INTERNET
48
48
48
CENTRAL
CONTROLLER
40 OR 94
MICROPROCESSOR
MEMORY
DISCONNECTED
FROM INTERNET
50 AND/
OR 50b AND/
OR 50 c
53
30, 31,
93 OR 93'
USER
49
PC1 AND/
OR 90 AND/
OR 501
INTERNET MALWARE FLUSHED AWAY : TEMPORARY MALWARE INFESTATION
LIMITED TO PUBLIC UNIT & ERASED BY CONTROLLED POWER INTERRUPTION

FIG. 10

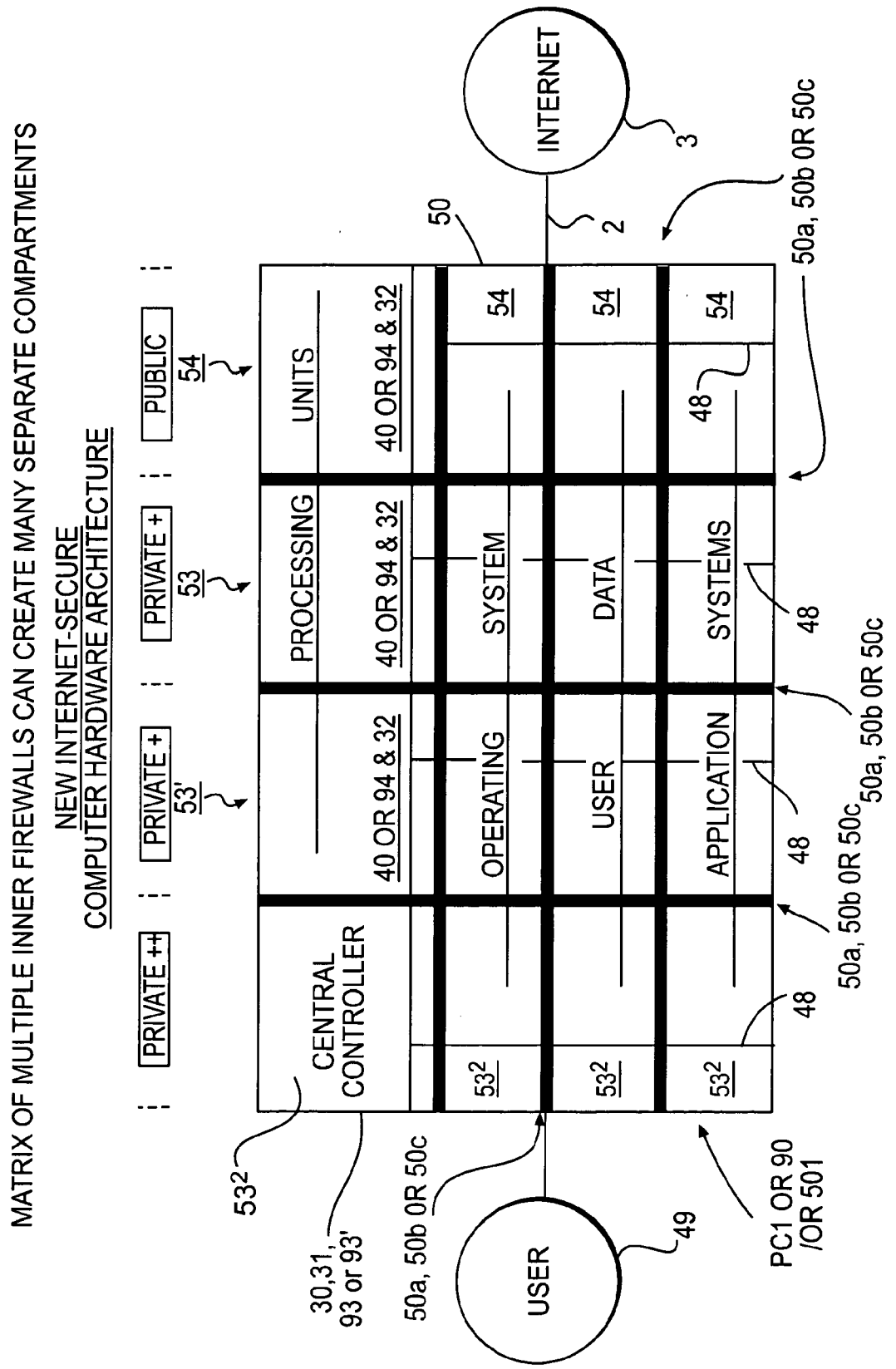
MATRIX OF MULTIPLE INNER FIREWALLS CAN CREATE MANY SEPARATE COMPARTMENTS
NEW INTERNET-SECURE
COMPUTER HARDWARE ARCHITECTURE
PRIVATE ++
PRIVATE +
PRIVATE +
PUBLIC
53'
53
54
INTERNET
3
2
50
50a, 50b OR 50c
CENTRAL CONTROLLER
PROCESSING UNITS
40 OR 94 & 32
OPERATING SYSTEM
USER DATA
APPLICATION SYSTEMS
48
532
30,31, 93 or 93'
50a, 50b OR 50c
USER
49
PC1 OR 90 /OR 501

FIG. 11

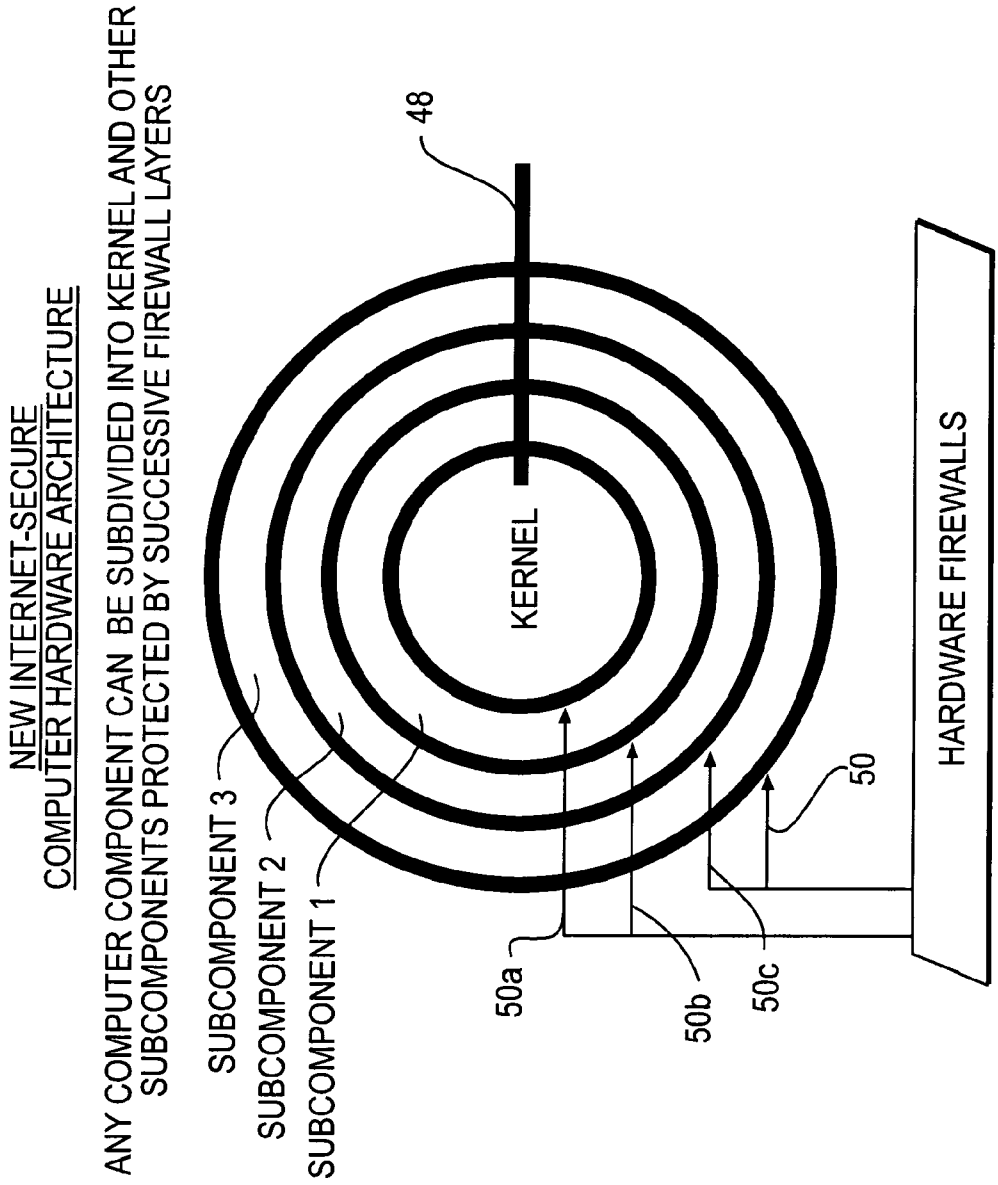
NEW INTERNET-SECURE
COMPUTER HARDWARE ARCHITECTURE
ANY COMPUTER COMPONENT CAN BE SUBDIVIDED INTO KERNEL AND OTHER SUBCOMPONENTS PROTECTED BY SUCCESSIVE FIREWALL LAYERS
SUBCOMPONENT 3
SUBCOMPONENT 2
SUBCOMPONENT 1
48
KERNEL
50a
50b
50c
50
HARDWARE FIREWALLS

FIG. 12

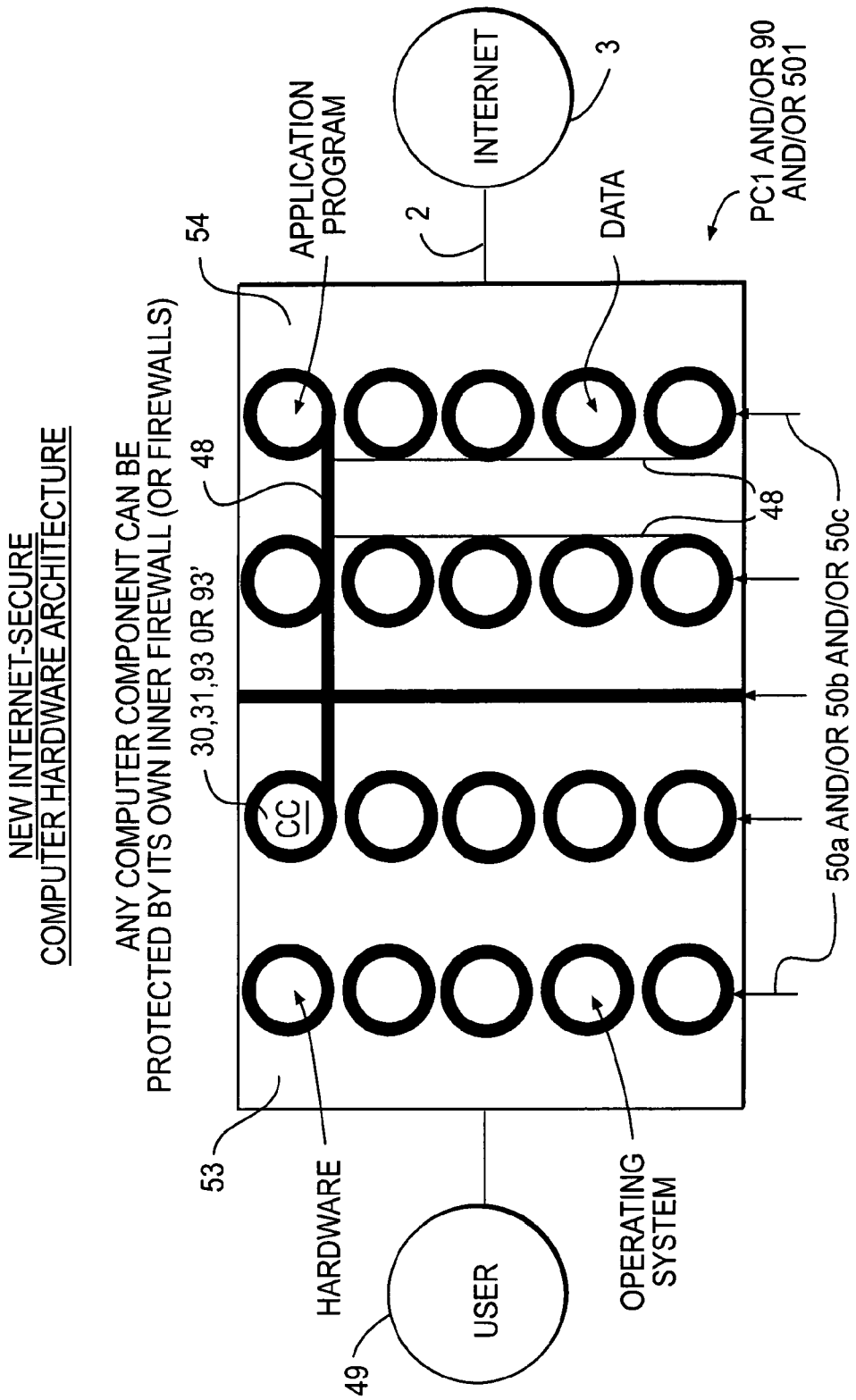
NEW INTERNET-SECURE
COMPUTER HARDWARE ARCHITECTURE
ANY COMPUTER COMPONENT CAN BE
PROTECTED BY ITS OWN INNER FIREWALL (OR FIREWALLS)
30,31,93 OR 93'
48
54
APPLICATION PROGRAM
INTERNET
3
2
DATA
PC1 AND/OR 90
AND/OR 501
48
50a AND/OR 50b AND/OR 50c
CC
53
HARDWARE
OPERATING SYSTEM
USER
49

FIG. 13

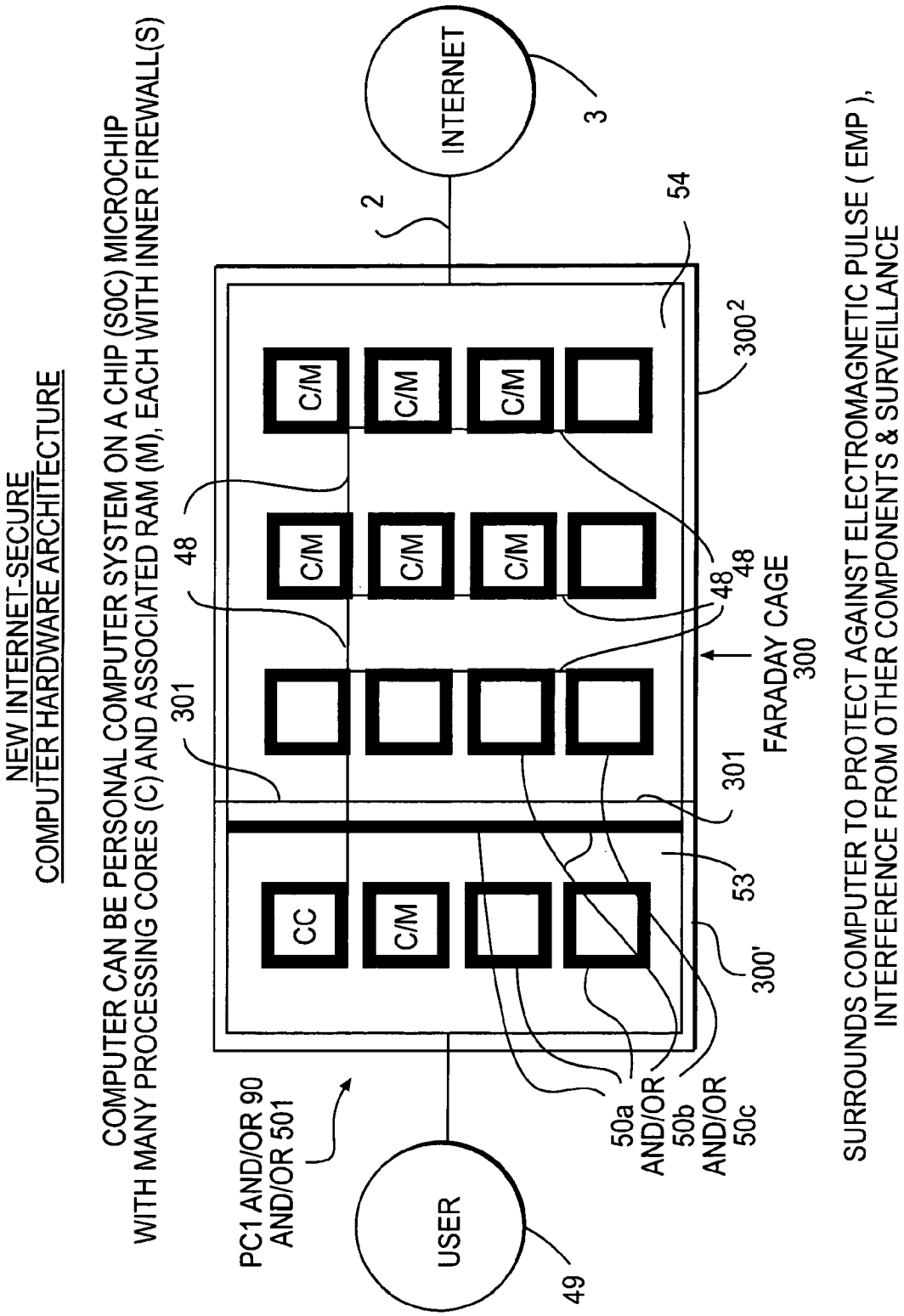
NEW INTERNET-SECURE
COMPUTER HARDWARE ARCHITECTURE
COMPUTER CAN BE PERSONAL COMPUTER SYSTEM ON A CHIP (SOC) MICROCHIP
WITH MANY PROCESSING CORES (C) AND ASSOCIATED RAM (M), EACH WITH INNER FIREWALL(S)
INTERNET
3
2
54
300 2
C/M
CC
48
301
FARADAY CAGE
300
53
300'
PC1 AND/OR 90
AND/OR 501
USER
49
50a
AND/OR
50b
AND/OR
50c
SURROUNDS COMPUTER TO PROTECT AGAINST ELECTROMAGNETIC PULSE (EMP),
INTERFERENCE FROM OTHER COMPONENTS & SURVEILLANCE

FIG. 14

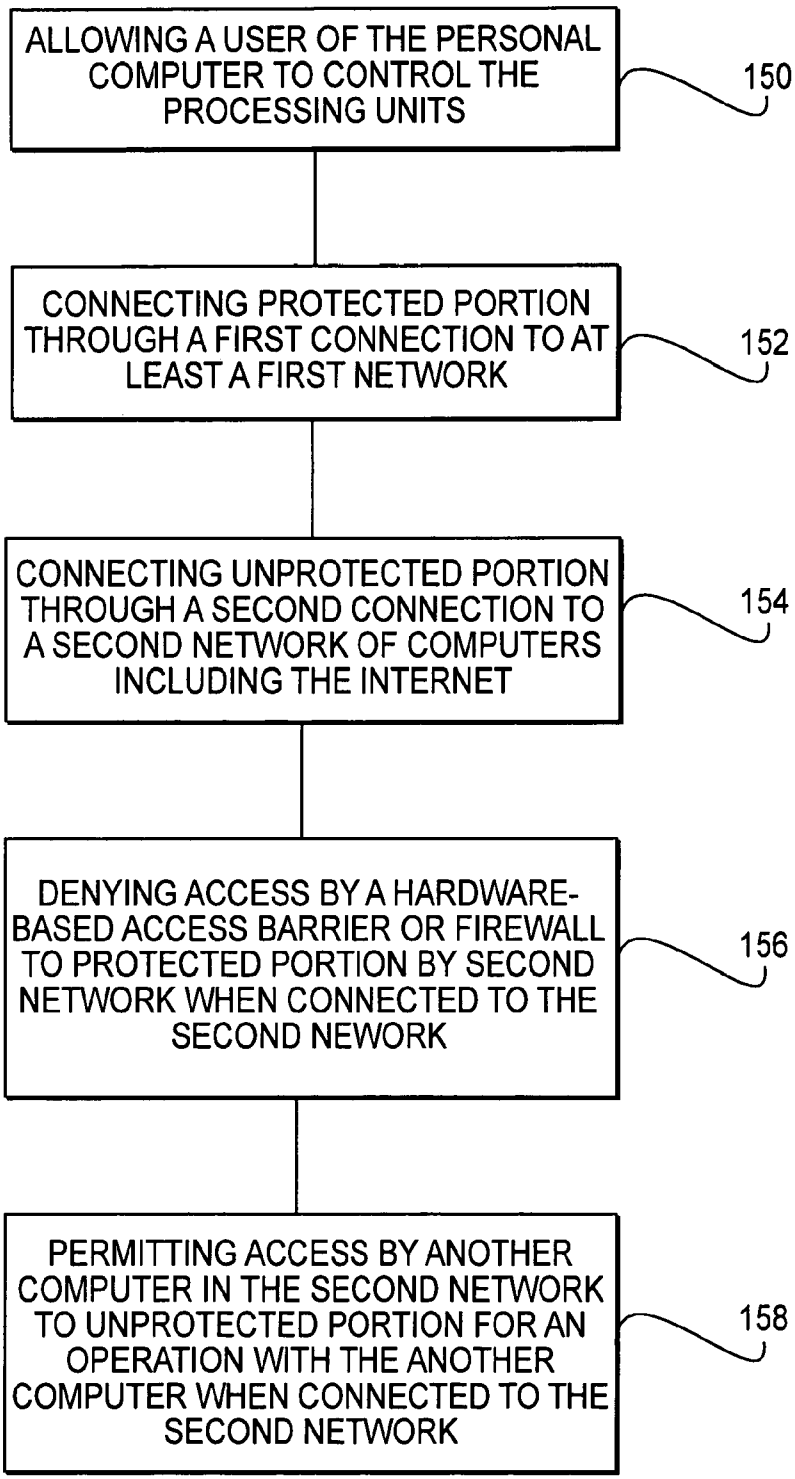
ALLOWING A USER OF THE PERSONAL COMPUTER TO CONTROL THE PROCESSING UNITS
150
CONNECTING PROTECTED PORTION THROUGH A FIRST CONNECTION TO AT LEAST A FIRST NETWORK
152
CONNECTING UNPROTECTED PORTION THROUGH A SECOND CONNECTION TO A SECOND NETWORK OF COMPUTERS INCLUDING THE INTERNET
154
DENYING ACCESS BY A HARDWARE-BASED ACCESS BARRIER OR FIREWALL TO PROTECTED PORTION BY SECOND NETWORK WHEN CONNECTED TO THE SECOND NEWORK
156
PERMITTING ACCESS BY ANOTHER COMPUTER IN THE SECOND NETWORK TO UNPROTECTED PORTION FOR AN OPERATION WITH THE ANOTHER COMPUTER WHEN CONNECTED TO THE SECOND NETWORK
158

FIG. 15

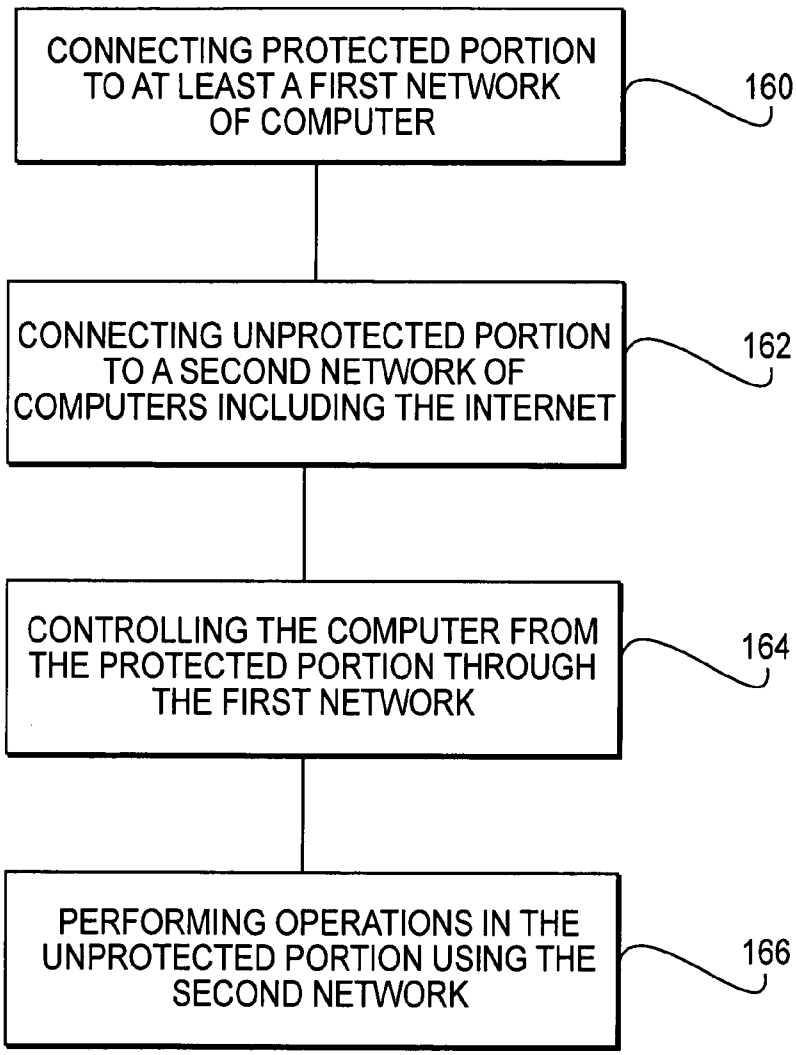
CONNECTING PROTECTED PORTION TO AT LEAST A FIRST NETWORK OF COMPUTER
160
CONNECTING UNPROTECTED PORTION TO A SECOND NETWORK OF COMPUTERS INCLUDING THE INTERNET
162
CONTROLLING THE COMPUTER FROM THE PROTECTED PORTION THROUGH THE FIRST NETWORK
164
PERFORMING OPERATIONS IN THE UNPROTECTED PORTION USING THE SECOND NETWORK
166

FIG. 16

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2011/023028

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 G06F21/00
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, COMPENDEX, INSPEC, PAJ, IBM-TDB, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2009/200661 A1 (ELLIS FRAMPTON E [US]) 13 August 2009 (2009-08-13) abstract paragraph [0086] - paragraph [0117] figures 10A, 10I	1-27
A	EP 1 164 766 A2 (IONOS CO LTD [JP]) 19 December 2001 (2001-12-19) abstract paragraph [0018] - paragraph [0021] paragraph [0029] - paragraph [0039] paragraph [0053] - paragraph [0072] figures 1, 5, 7-10	1-27

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 May 2011	19/05/2011

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Horn, Marc-Philipp

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2011/023028

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2007/162974 A1 (SPEIDEL THOMAS [DE]) 12 July 2007 (2007-07-12) abstract paragraph [0016] - paragraph [0029] figures 1, 2 -----	1-27
A	US 2004/098621 A1 (RAYMOND BRANDL [US]) 20 May 2004 (2004-05-20) abstract paragraph [0026] - paragraph [0032] figure 2 -----	1-27

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2011/023028

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2009200661 A1	13-08-2009	NONE	
EP 1164766 A2	19-12-2001	DE 60117200 T2	23-11-2006
		JP 2002007233 A	11-01-2002
		US 2001054159 A1	20-12-2001
US 2007162974 A1	12-07-2007	AT 410722 T	15-10-2008
		EP 1742135 A1	10-01-2007
US 2004098621 A1	20-05-2004	NONE	