US008171537B2

(12) **United States Patent**
Ellis

(10) **Patent No.: US 8,171,537 B2**
(45) **Date of Patent: May 1, 2012**

(54) **METHOD OF SECURELY CONTROLLING THROUGH ONE OR MORE SEPARATE PRIVATE NETWORKS AN INTERNET-CONNECTED COMPUTER HAVING ONE OR MORE HARDWARE-BASED INNER FIREWALLS OR ACCESS BARRIERS**

(76) Inventor: **Frampton E. Ellis**, Jasper, FL (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **13/016,527**

(22) Filed: **Jan. 28, 2011**

(65) **Prior Publication Data**

US 2011/0231926 A1 Sep. 22, 2011

Related U.S. Application Data

(60) Provisional application No. 61/282,378, filed on Jan. 29, 2010, provisional application No. 61/282,478, filed on Feb. 17, 2010, provisional application No. 61/282,503, filed on Feb. 22, 2010, provisional application No. 61/282,861, filed on Apr. 12, 2010, provisional application No. 61/344,018, filed on May 7, 2010, provisional application No. 61/457,184, filed on Jan. 24, 2011.

(51) **Int. Cl.**
G06F 15/173 (2006.01)
G06F 13/40 (2006.01)
G06F 17/00 (2006.01)

(52) **U.S. Cl.** **726/11**; 726/22; 726/30; 713/194

(58) **Field of Classification Search** 726/11, 726/22, 30; 713/194
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,550,984	A	8/1996	Gelb
5,802,320	A	9/1998	Baehr et al.
5,896,499	A	4/1999	McKelvey
6,167,428	A	12/2000	Ellis
6,202,153	B1	3/2001	Diamant et al.

(Continued)

FOREIGN PATENT DOCUMENTS

EP 1 164 766 A2 12/2001

OTHER PUBLICATIONS

Connect One. "iChip CO2064/CO2128/CO2144 Data Sheet Ver. 1.20", 2011.*

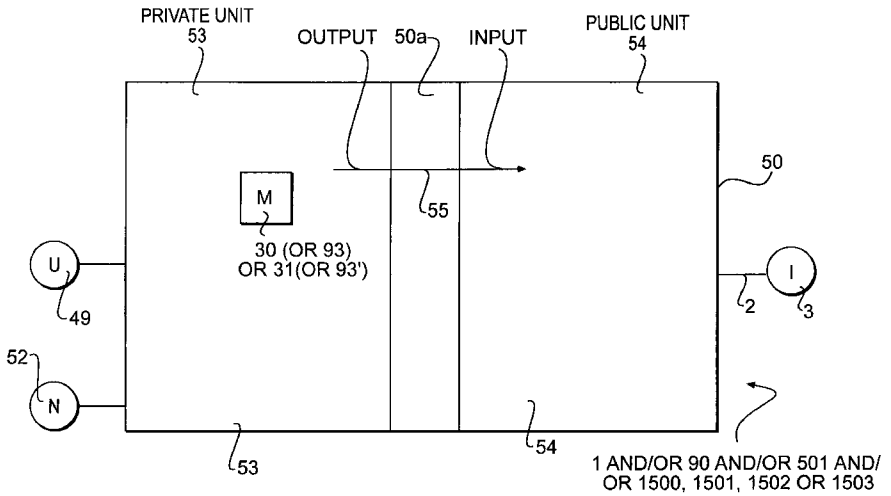
(Continued)

Primary Examiner — Michael Simitoski
(74) *Attorney, Agent, or Firm* — Finnegan, Henderson, Farabow, Garrett & Dunner LLP

(57) **ABSTRACT**

A method of securely controlling through a private network a computer protected by a hardware-based inner access barrier or firewall and configured to operate as a general purpose computer connected to the Internet, comprising: two separate network connections separated by an inner hardware-based access barrier or inner hardware-based firewall protecting a private network connection configured for connection to a private network of computers but not protecting a public network connection configured for connection to a public network configured to include the Internet, the method including the step of controlling at least one operation of the computer, the control being provided through the private network and the operation involving data and/or code transmitted through an out-only bus or channel. Another method includes the step of controlling an operation of a second or third private protected unit of the computer, the control being provided through a second or third private network, respectively.

29 Claims, 16 Drawing Sheets



U.S. PATENT DOCUMENTS

6,725,250	B1	4/2004	Ellis
6,732,141	B2	5/2004	Ellis
7,024,449	B1	4/2006	Ellis
7,035,906	B1	4/2006	Ellis
7,047,275	B1	5/2006	Ellis
7,467,406	B2	12/2008	Cox et al.
7,506,020	B2	3/2009	Ellis
7,562,211	B2	7/2009	Paya et al.
7,606,854	B2	10/2009	Ellis
7,634,529	B2	12/2009	Ellis
7,805,756	B2	9/2010	Ellis
7,814,233	B2	10/2010	Ellis
7,840,997	B2	11/2010	Shevchenko
7,908,650	B2	3/2011	Ellis
7,926,097	B2	4/2011	Ellis
7,984,301	B2	7/2011	Kaabouch et al.
8,010,789	B2	8/2011	Witchey
2001/0054159	A1	12/2001	Hishino
2004/0073603	A1	4/2004	Ellis
2004/0098621	A1	5/2004	Raymond
2004/0158744	A1	8/2004	Deng et al.
2004/0162992	A1	8/2004	Sami et al.
2004/0215931	A1	10/2004	Ellis
2006/0095497	A1	5/2006	Ellis
2006/0177226	A1	8/2006	Ellis
2006/0190565	A1	8/2006	Ellis
2007/0162974	A1	7/2007	Speidel
2007/0300305	A1	12/2007	Gonsalves et al.
2008/0134290	A1	6/2008	Olsson
2009/0031412	A1	1/2009	Ellis
2009/0200661	A1	8/2009	Ellis
2009/0254986	A1	10/2009	Harris et al.
2009/0282092	A1	11/2009	Ellis
2010/0011083	A1	1/2010	Ellis
2011/0004930	A1	1/2011	Ellis
2011/0004931	A1	1/2011	Ellis

OTHER PUBLICATIONS

Shao, Fengjing et al. "A New Secure Architecture of Network Computer Based on Single CPU and Dual Bus", Fifth IEEE International Symposium on Embedded Computing, 2008.*

Wang, Tiedong et al. "A Hardware Implement of Bus Bridge Based on Single CPU and Dual Bus", 2008 International Symposium on Computer Science and Computational Technology, 2008.*

International Search Report and Written Opinion for PCT/US 2011/025257, dated May 19, 2011.

* cited by examiner

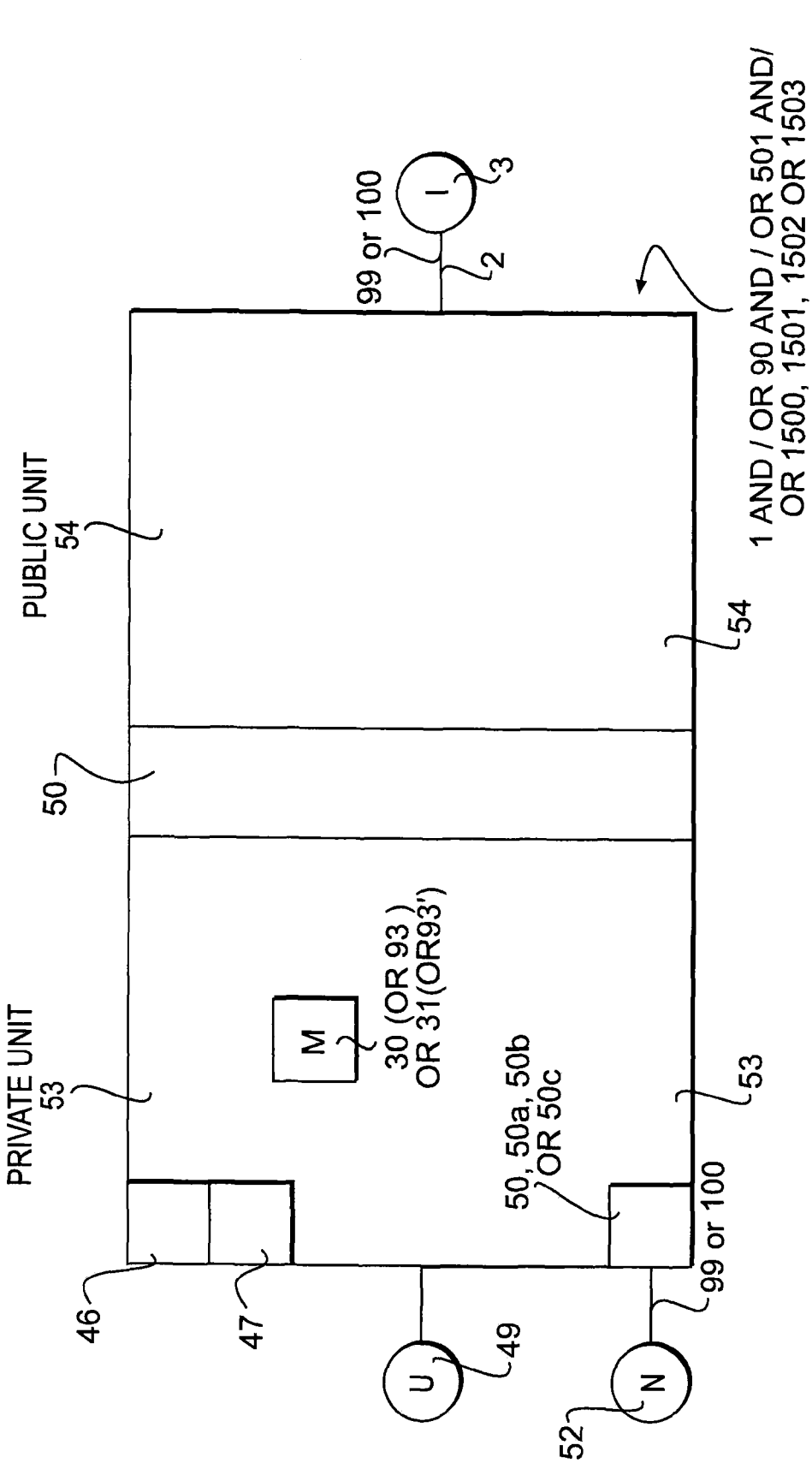

PUBLIC UNIT
54
PRIVATE UNIT
53
50
99 or 100
I
3
2
1 AND / OR 90 AND / OR 501 AND/
OR 1500, 1501, 1502 OR 1503
54
53
M
30 (OR 93)
OR 31(OR93')
50, 50a, 50b
OR 50c
99 or 100
46
47
U
49
N
52

FIG. 1

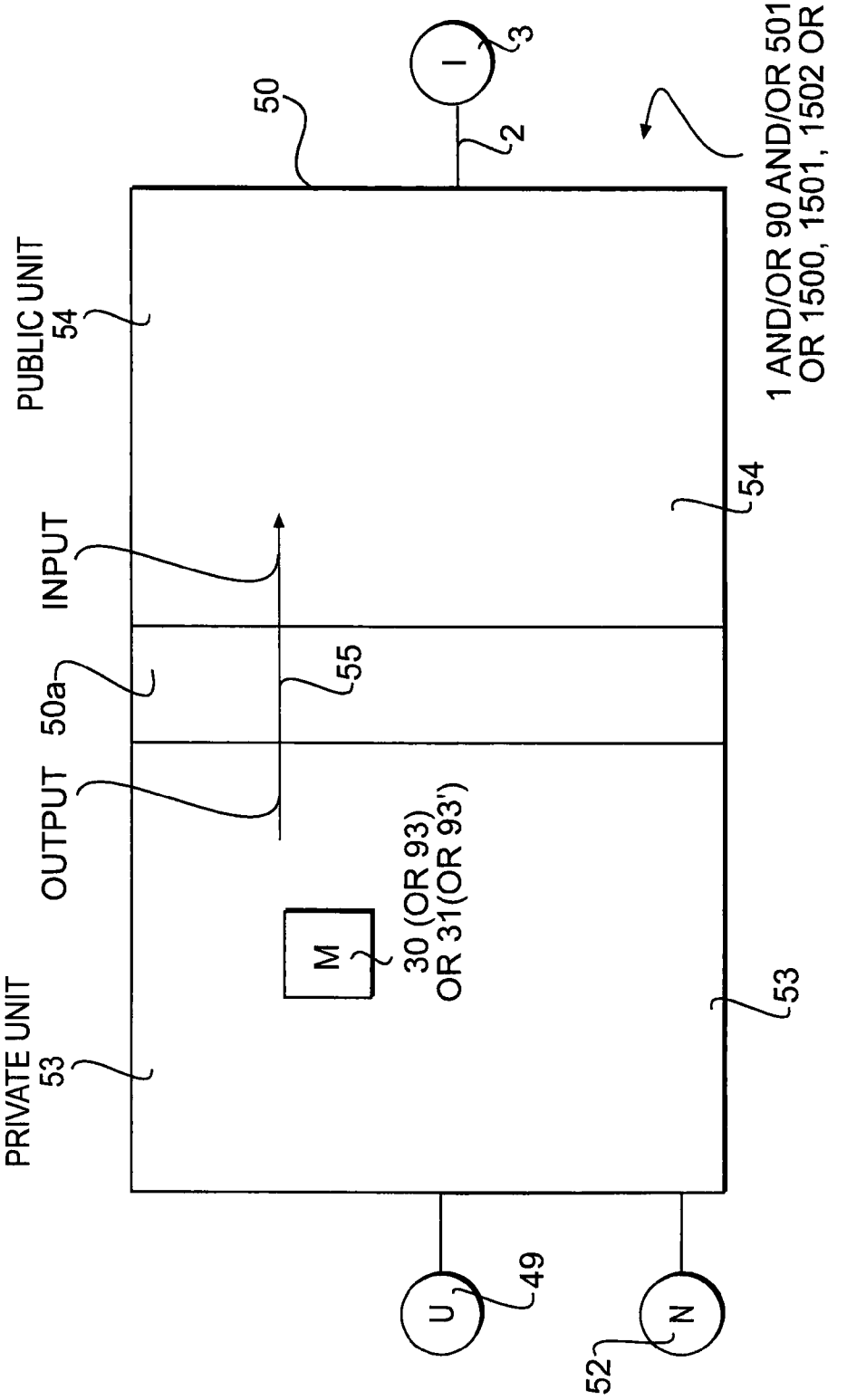

PUBLIC UNIT
54
INPUT
50a
OUTPUT
PRIVATE UNIT
53
50
I
3
2
1 AND/OR 90 AND/OR 501 AND/
OR 1500, 1501, 1502 OR 1503
54
55
M
30 (OR 93)
OR 31(OR 93')
53
U
49
N
52

FIG. 2

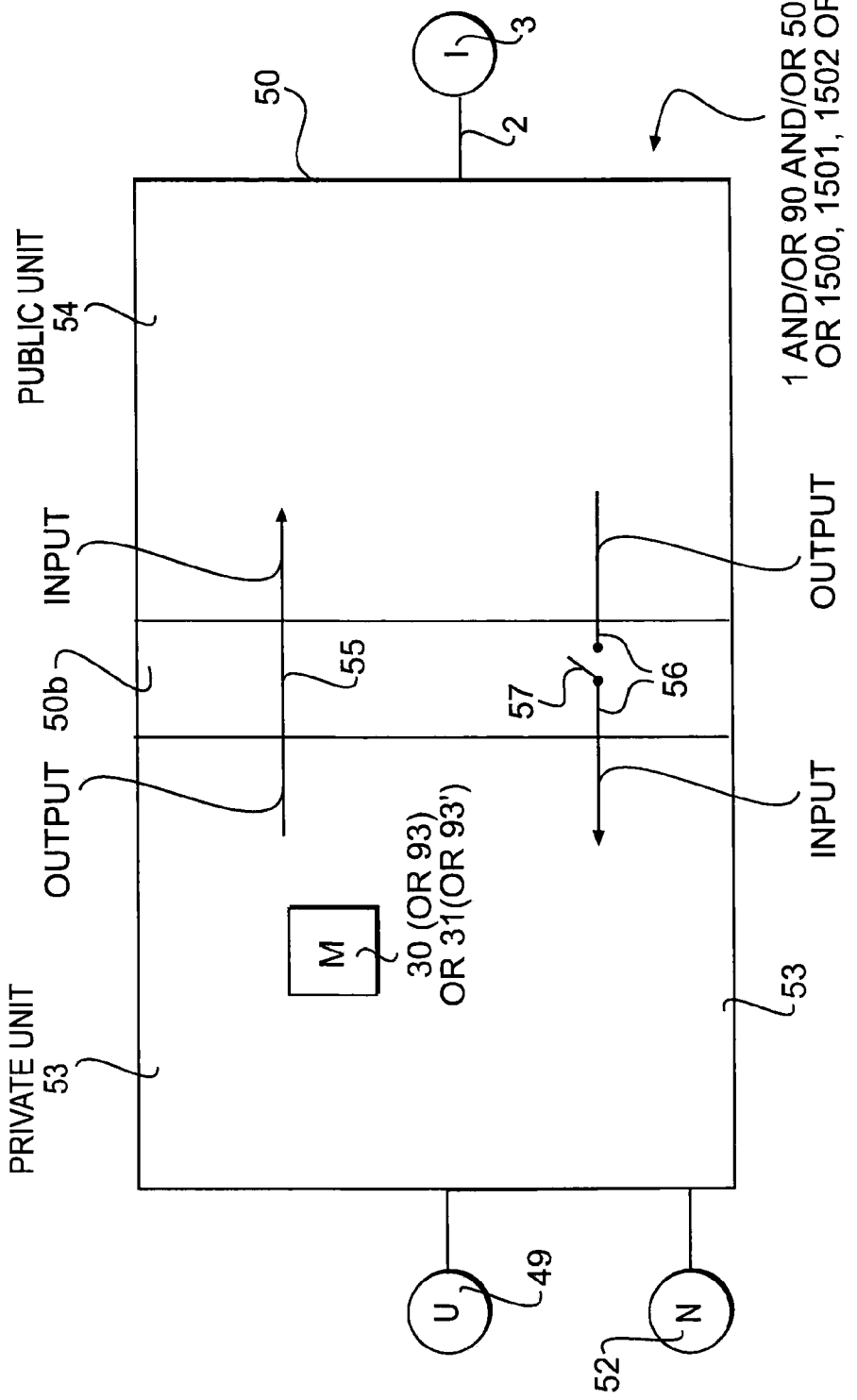

1 AND/OR 90 AND/OR 505 AND/
OR 1500, 1501, 1502 OR 1503
50
I
3
2
PUBLIC UNIT
54
INPUT
OUTPUT
50b
55
57
56
OUTPUT
INPUT
M
30 (OR 93)
OR 31(OR 93')
PRIVATE UNIT
53
53
U
49
N
52

FIG. 3

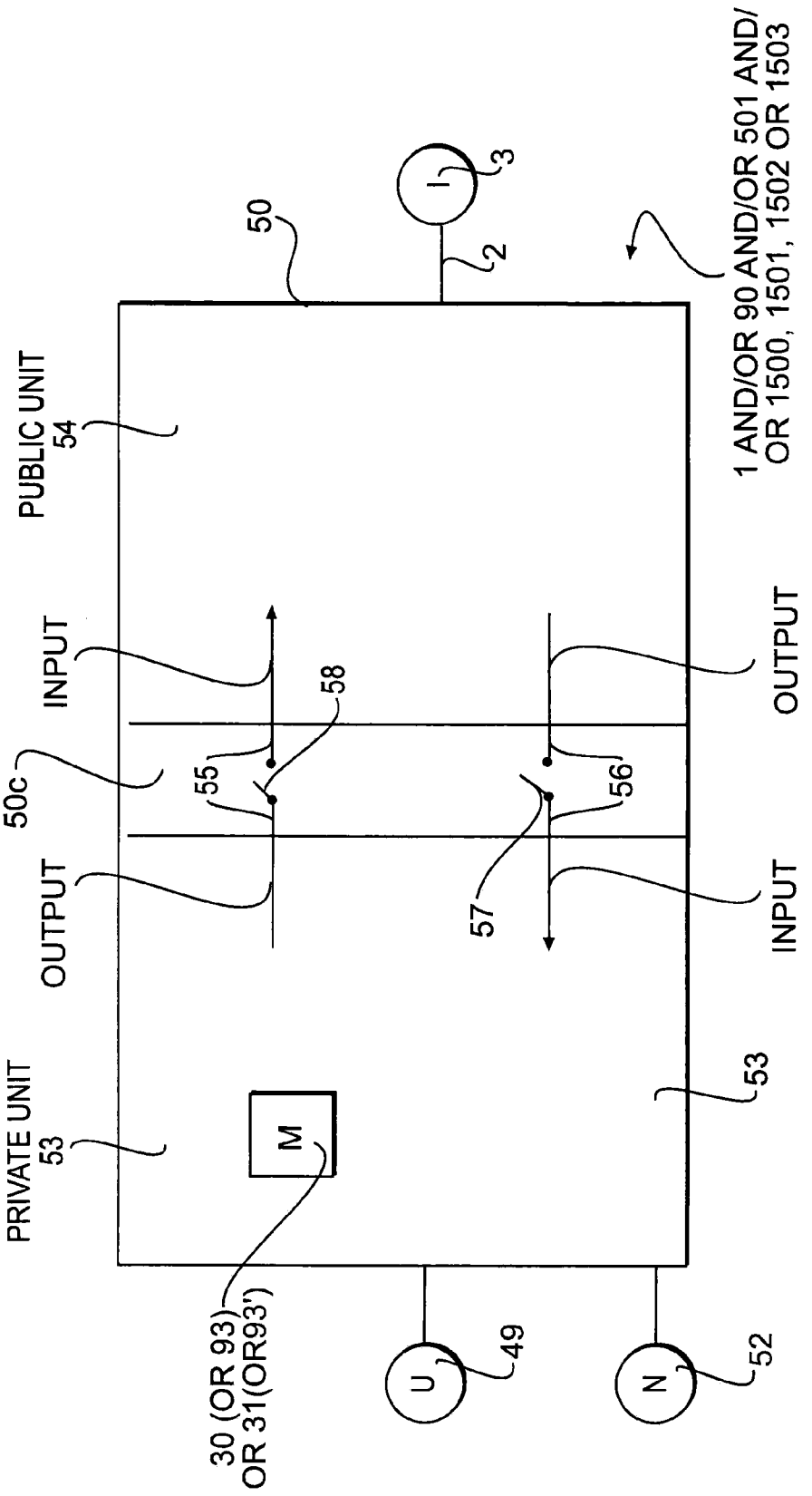

1 AND/OR 90 AND/OR 501 AND/
OR 1500, 1501, 1502 OR 1503
50
I
3
2
PUBLIC UNIT
54
INPUT
OUTPUT
58
55
50c
56
57
OUTPUT
INPUT
PRIVATE UNIT
53
M
53
30 (OR 93)
OR 31(OR93')
U
49
N
52

FIG. 4

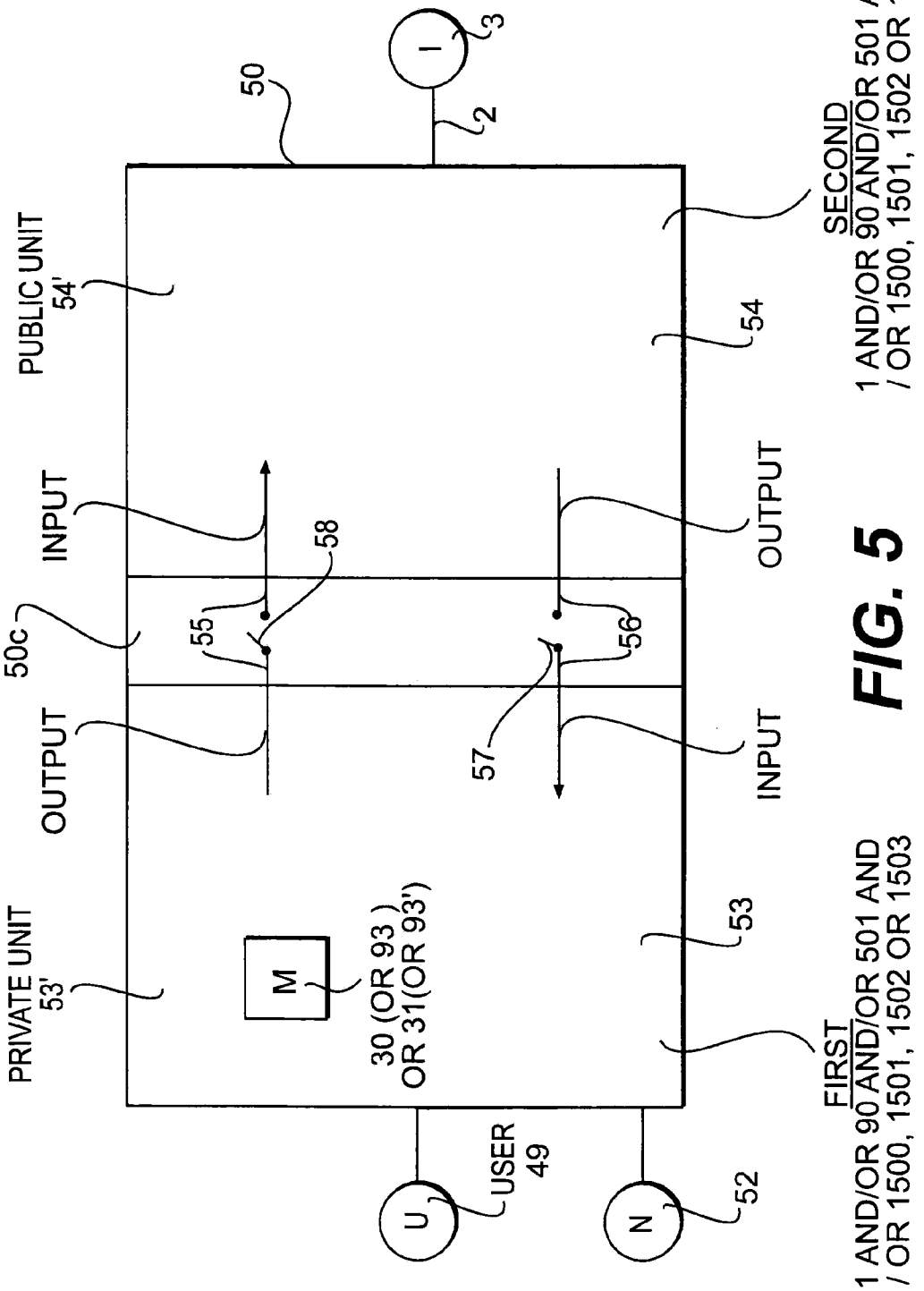

50
I
3
2
PUBLIC UNIT
54'
INPUT
58
55
50c
OUTPUT
PRIVATE UNIT
53'
M
30 (OR 93)
OR 31(OR 93')
U
USER
49
N
52
53
54
SECOND
1 AND/OR 90 AND/OR 501 AND
/ OR 1500, 1501, 1502 OR 1503
OUTPUT
56
57
INPUT
FIRST
1 AND/OR 90 AND/OR 501 AND
/ OR 1500, 1501, 1502 OR 1503

FIG. 5

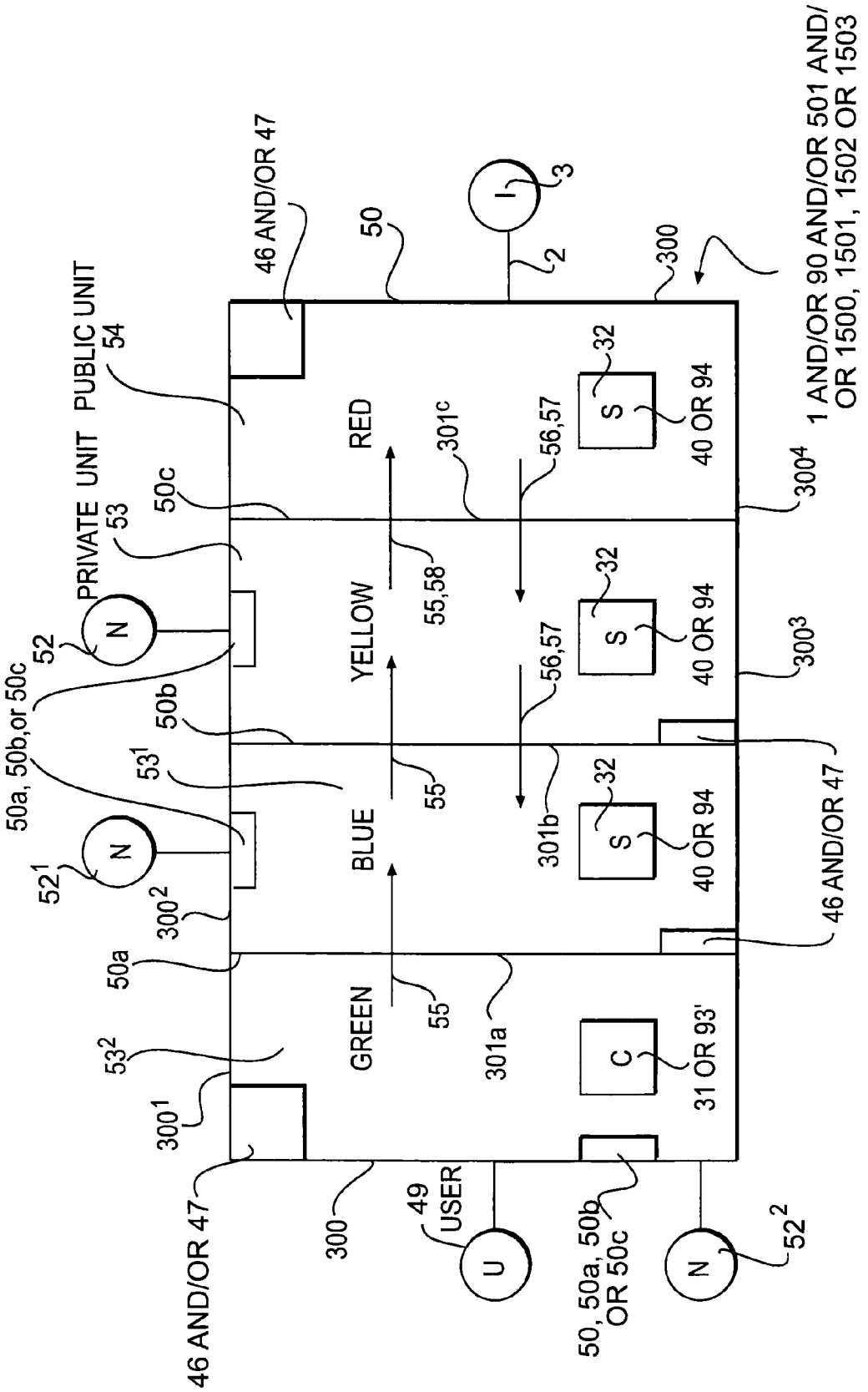

46 AND/OR 47
300
49 USER
U
50, 50a, 50b OR 50c
N
52²
300¹
53²
50a
300²
52¹
N
50a, 50b, or 50c
53¹
50b
52
N
PRIVATE UNIT
53
50c
PUBLIC UNIT
54
46 AND/OR 47
50
I
2
3
300
1 AND/OR 90 AND/OR 501 AND/ OR 1500, 1501, 1502 OR 1503
300⁴
300³
46 AND/OR 47
GREEN
BLUE
YELLOW
RED
55
55
55,58
301a
301b
301c
56,57
56,57
C
S
S
S
S
31 OR 93'
40 OR 94
40 OR 94
40 OR 94
32
32
32

FIG. 6

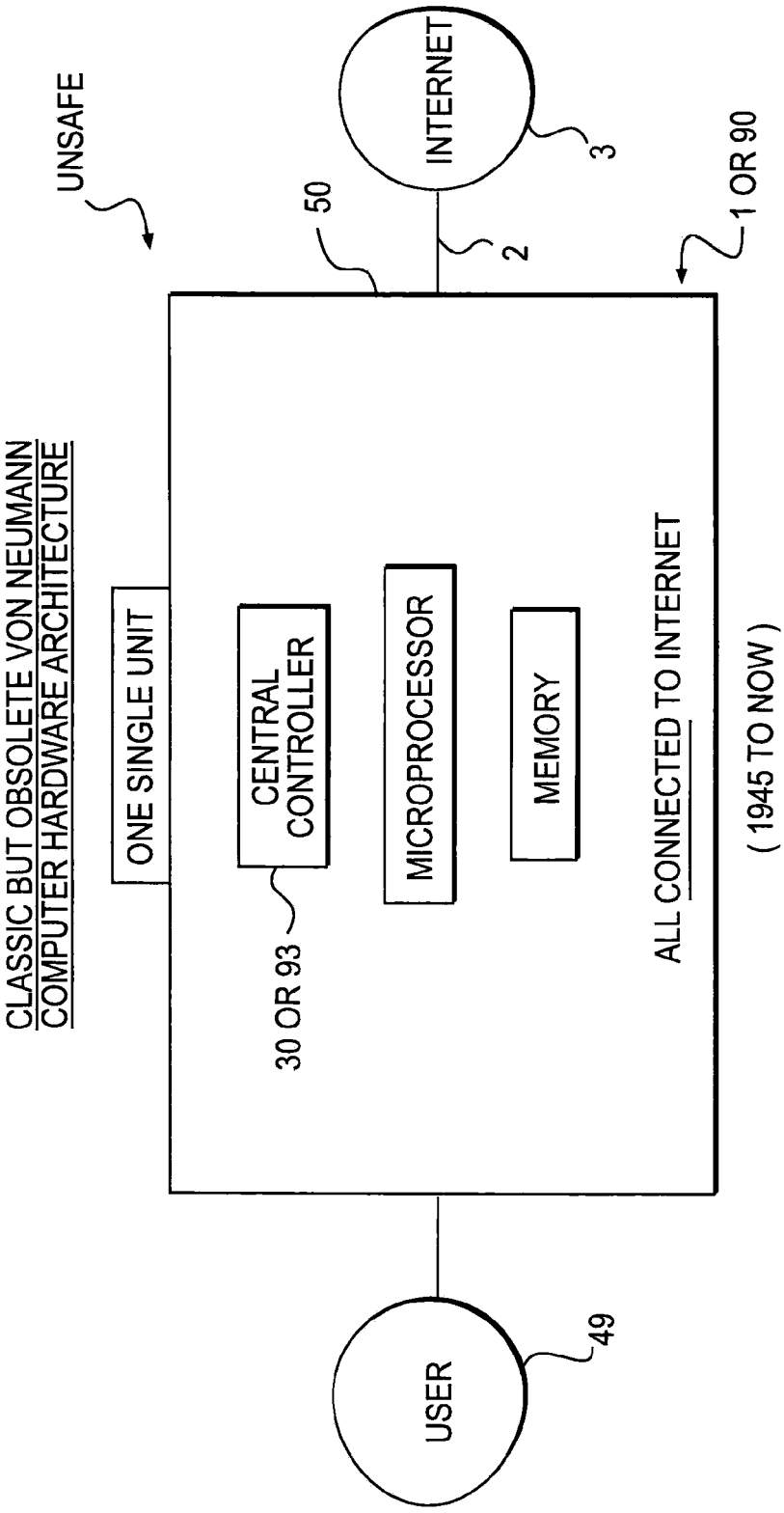

CLASSIC BUT OBSOLETE VON NEUMANN
COMPUTER HARDWARE ARCHITECTURE
UNSAFE
INTERNET
3
50
2
1 OR 90
ONE SINGLE UNIT
CENTRAL CONTROLLER
30 OR 93
MICROPROCESSOR
MEMORY
ALL CONNECTED TO INTERNET
(1945 TO NOW)
USER
49
THE PROBLEM: INTERNET MALWARE HAS POTENTIAL ACCESS
TO ENTIRE COMPUTER TO CONTROL ANY PART OR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

FIG. 7

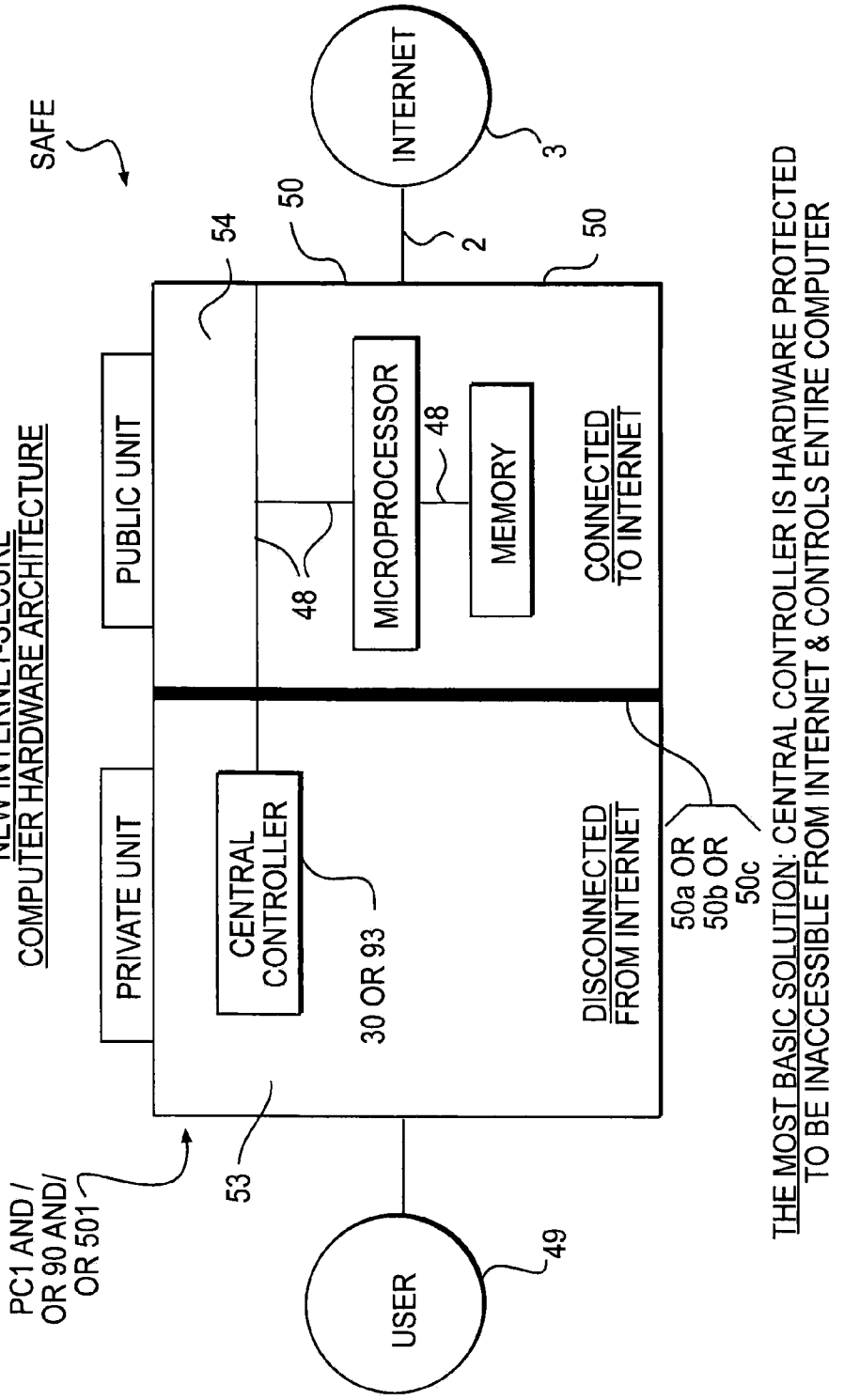

NEW INTERNET-SECURE
COMPUTER HARDWARE ARCHITECTURE
SAFE
INTERNET
3
2
50
50
54
PUBLIC UNIT
PRIVATE UNIT
MICROPROCESSOR
48
48
MEMORY
CONNECTED
TO INTERNET
CENTRAL
CONTROLLER
30 OR 93
DISCONNECTED
FROM INTERNET
50a OR
50b OR
50c
PC1 AND /
OR 90 AND/
OR 501
53
USER
49
THE MOST BASIC SOLUTION: CENTRAL CONTROLLER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

FIG. 8

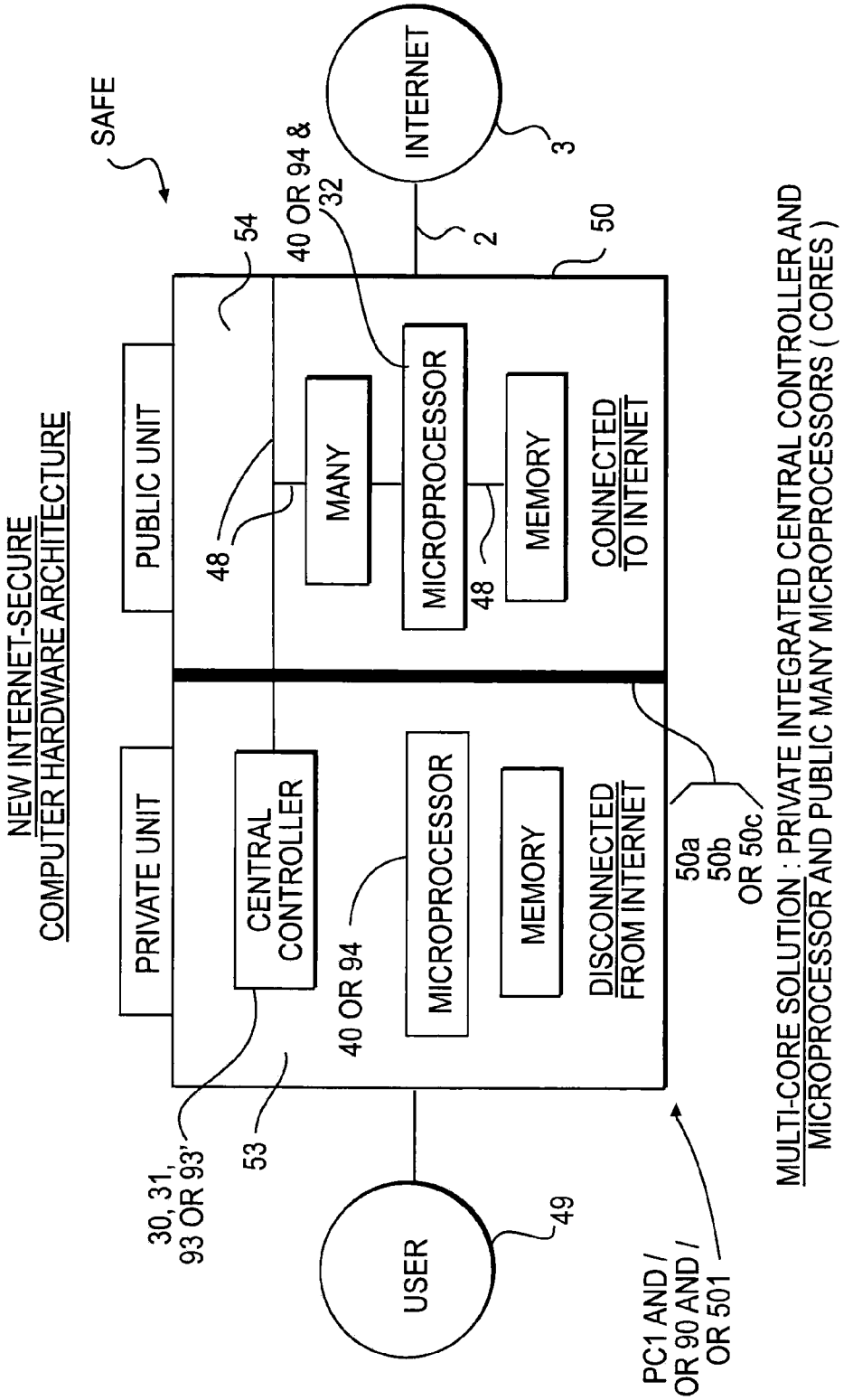

NEW INTERNET-SECURE
COMPUTER HARDWARE ARCHITECTURE
SAFE
INTERNET
3
2
54
40 OR 94 &
32
50
PUBLIC UNIT
PRIVATE UNIT
48
MANY
MICROPROCESSOR
48
MEMORY
CONNECTED
TO INTERNET
CENTRAL
CONTROLLER
40 OR 94
MICROPROCESSOR
MEMORY
DISCONNECTED
FROM INTERNET
50a
50b
OR 50c
30, 31,
93 OR 93'
53
USER
49
PC1 AND /
OR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

FIG. 9

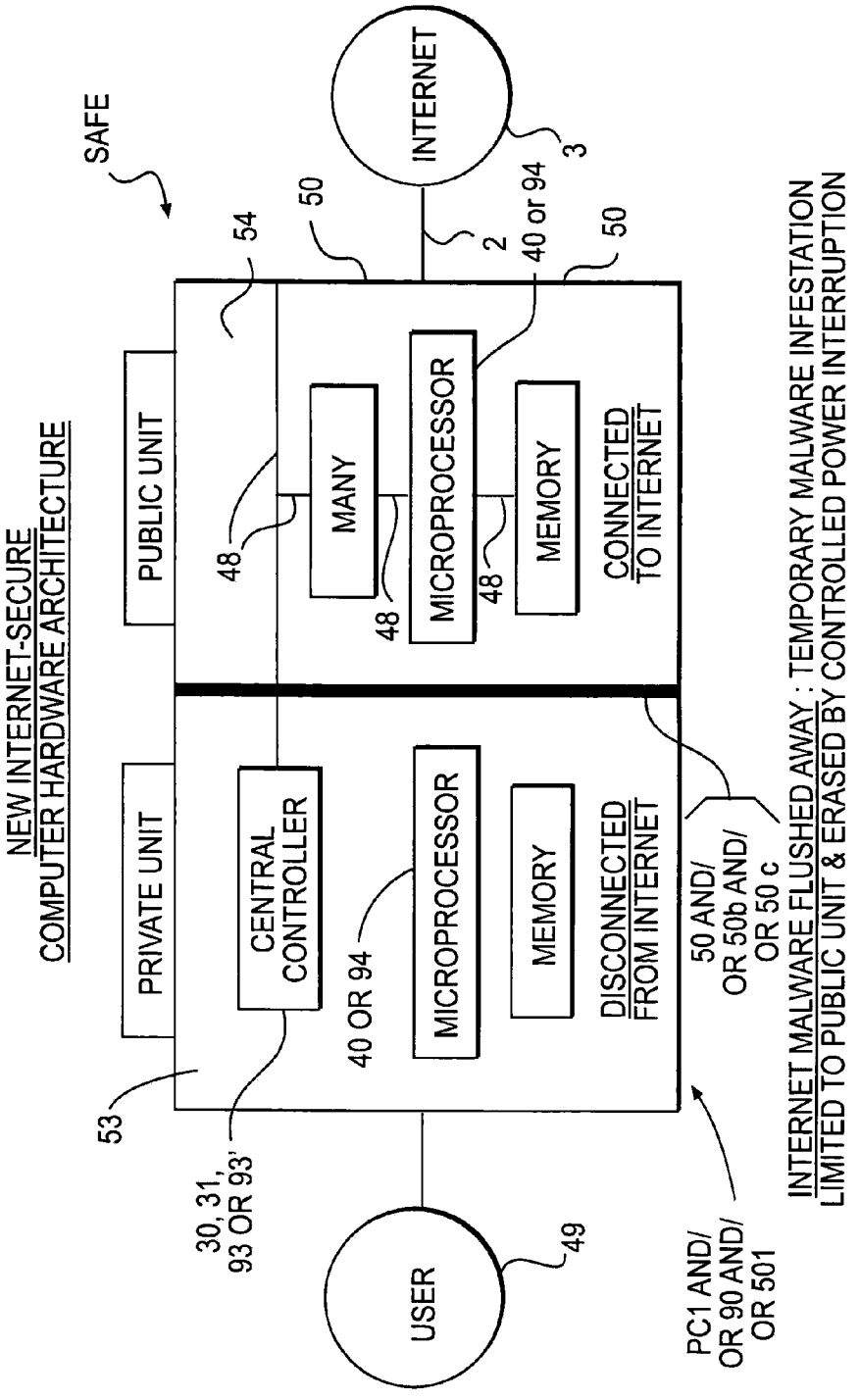

NEW INTERNET-SECURE
COMPUTER HARDWARE ARCHITECTURE
SAFE
PUBLIC UNIT
PRIVATE UNIT
INTERNET
3
2
40 or 94
50
54
48
MANY
MICROPROCESSOR
MEMORY
CONNECTED
TO INTERNET
CENTRAL
CONTROLLER
40 OR 94
MICROPROCESSOR
MEMORY
DISCONNECTED
FROM INTERNET
50 AND/
OR 50b AND/
OR 50 c
53
30, 31,
93 OR 93'
USER
49
PC1 AND/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

FIG. 10

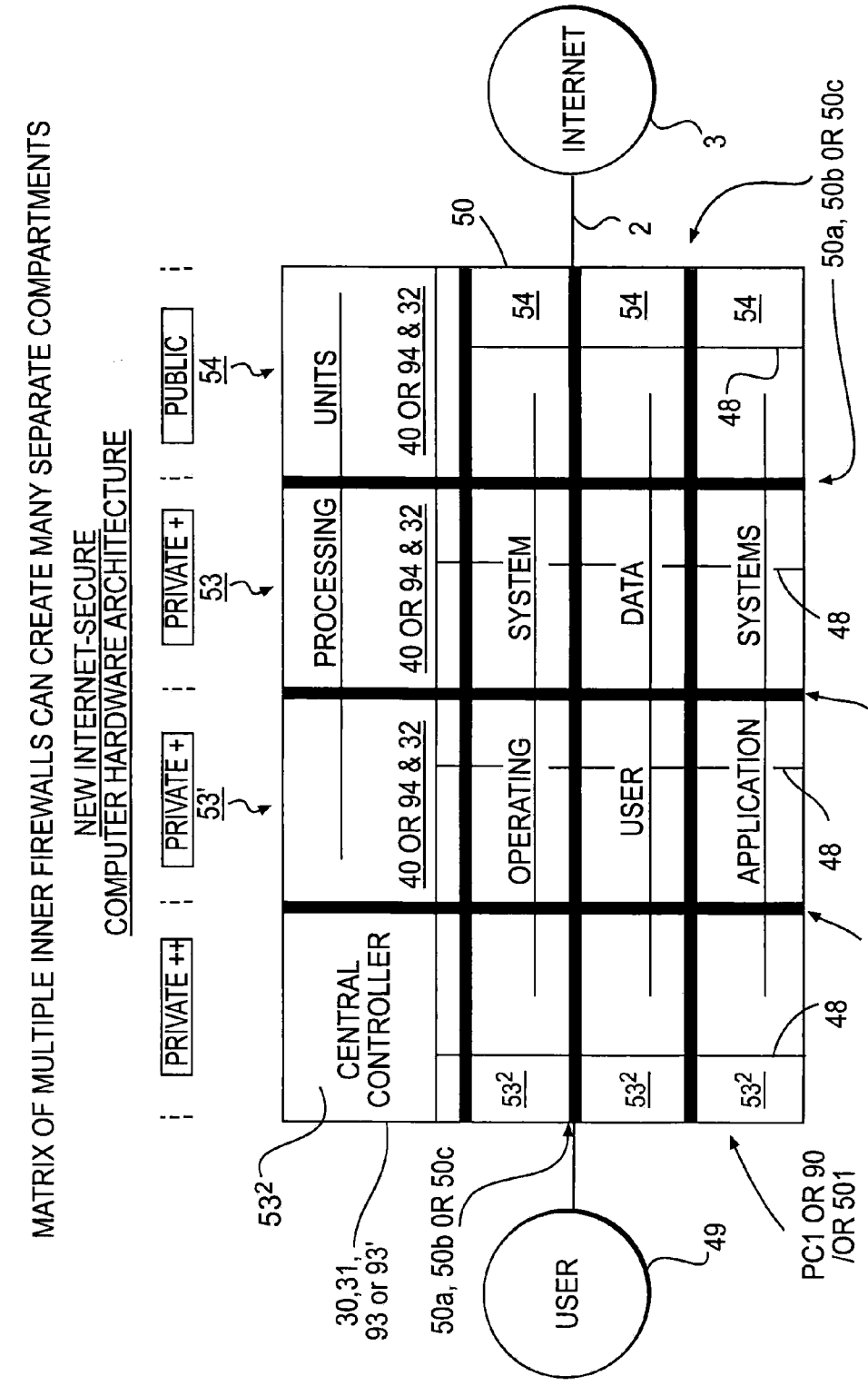

MATRIX OF MULTIPLE INNER FIREWALLS CAN CREATE MANY SEPARATE COMPARTMENTS
NEW INTERNET-SECURE
COMPUTER HARDWARE ARCHITECTURE
PRIVATE ++
PRIVATE +
PRIVATE +
PUBLIC
53'
53
54
CENTRAL CONTROLLER
PROCESSING UNITS
40 OR 94 & 32
OPERATING SYSTEM
USER DATA
APPLICATION SYSTEMS
532
30,31, 93 or 93'
50a, 50b OR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

FIG. 11

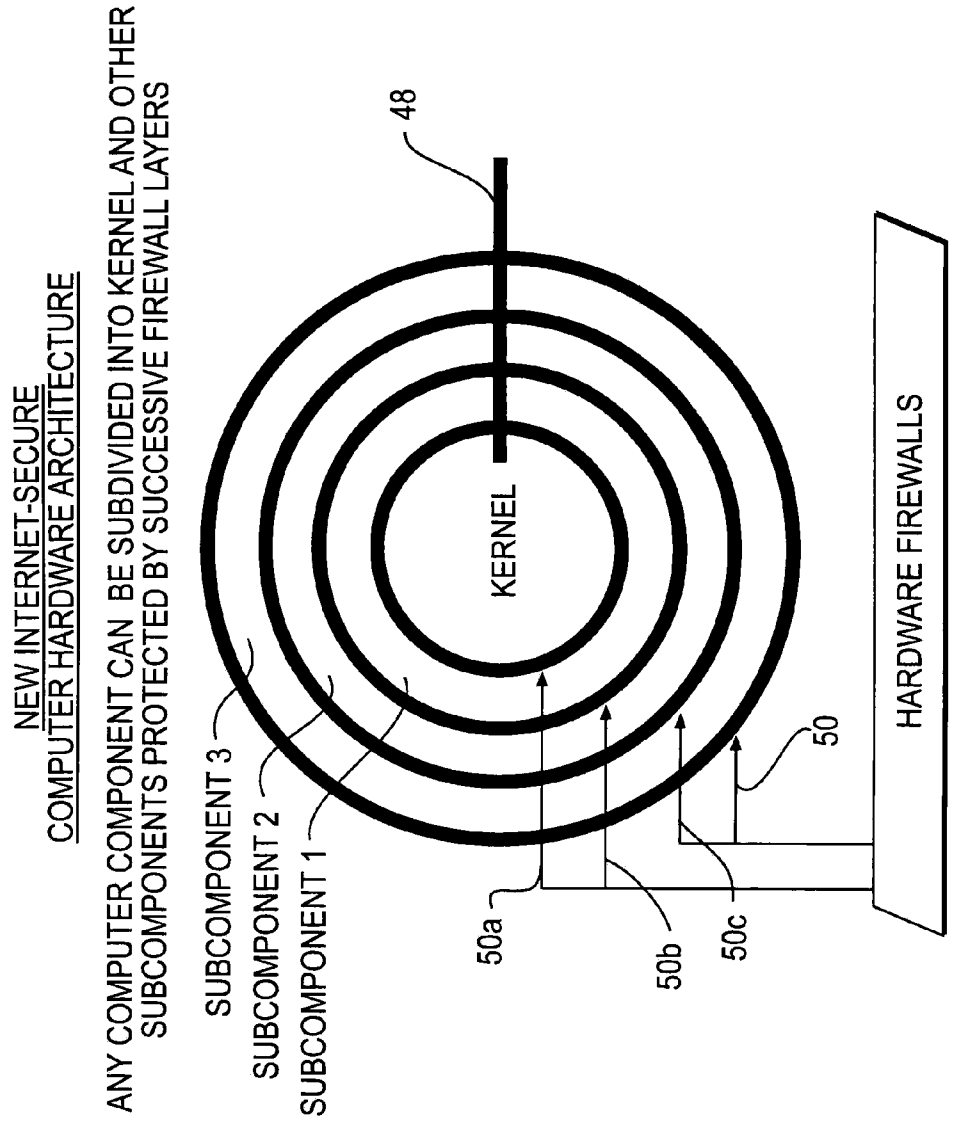

NEW INTERNET-SECURE
COMPUTER HARDWARE ARCHITECTURE
ANY COMPUTER COMPONENT CAN BE SUBDIVIDED INTO KERNEL AND OTHER SUBCOMPONENTS PROTECTED BY SUCCESSIVE FIREWALL LAYERS
SUBCOMPONENT 3
SUBCOMPONENT 2
SUBCOMPONENT 1
KERNEL
48
50a
50b
50c
50
HARDWARE FIREWALLS

FIG. 12

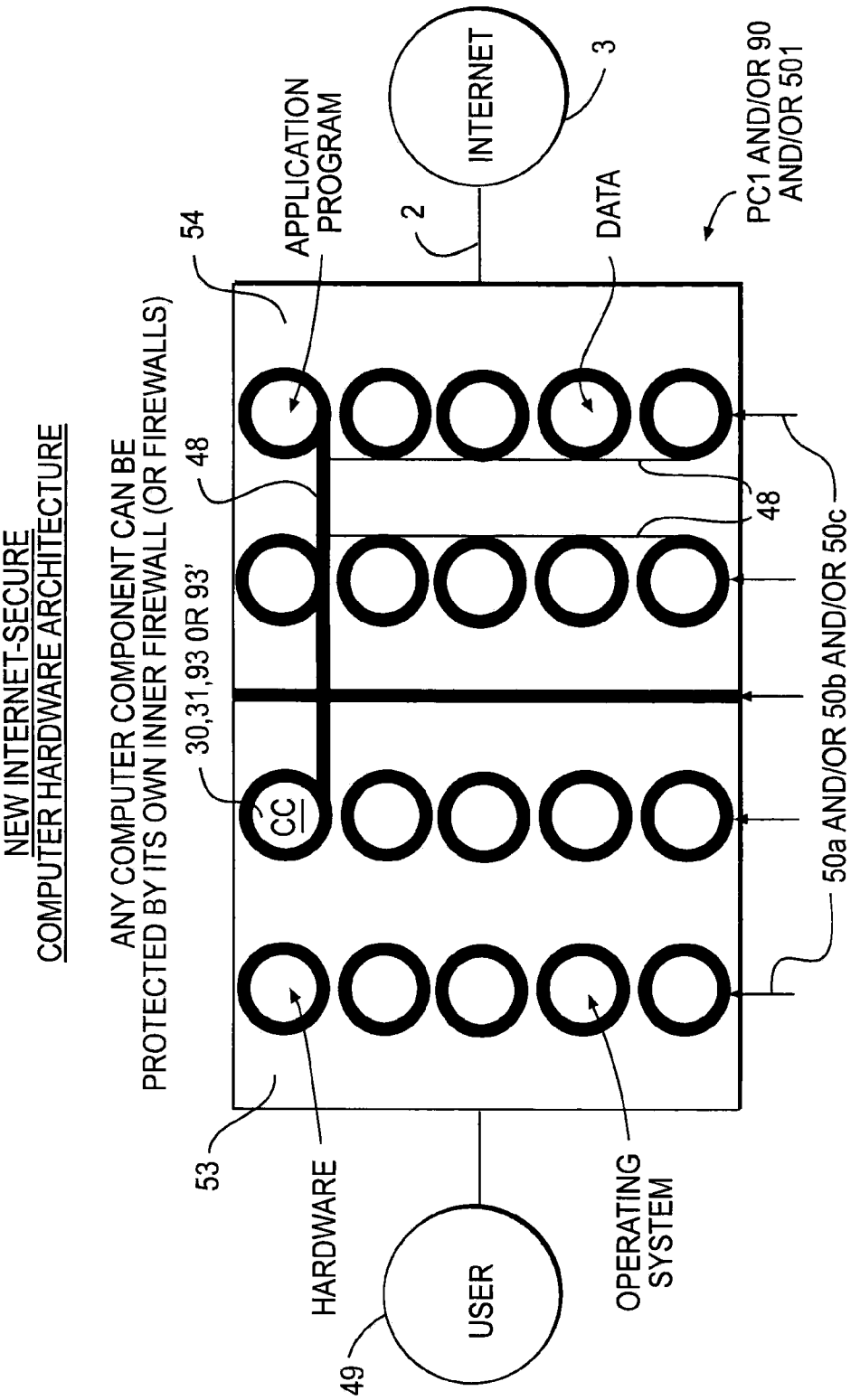

NEW INTERNET-SECURE
COMPUTER HARDWARE ARCHITECTURE
ANY COMPUTER COMPONENT CAN BE
PROTECTED BY ITS OWN INNER FIREWALL (OR FIREWALLS)
30,31,93 OR 93'
48
54
APPLICATION PROGRAM
INTERNET
3
2
DATA
PC1 AND/OR 90
AND/OR 501
48
50a AND/OR 50b AND/OR 50c
CC
53
HARDWARE
USER
49
OPERATING SYSTEM

FIG. 13

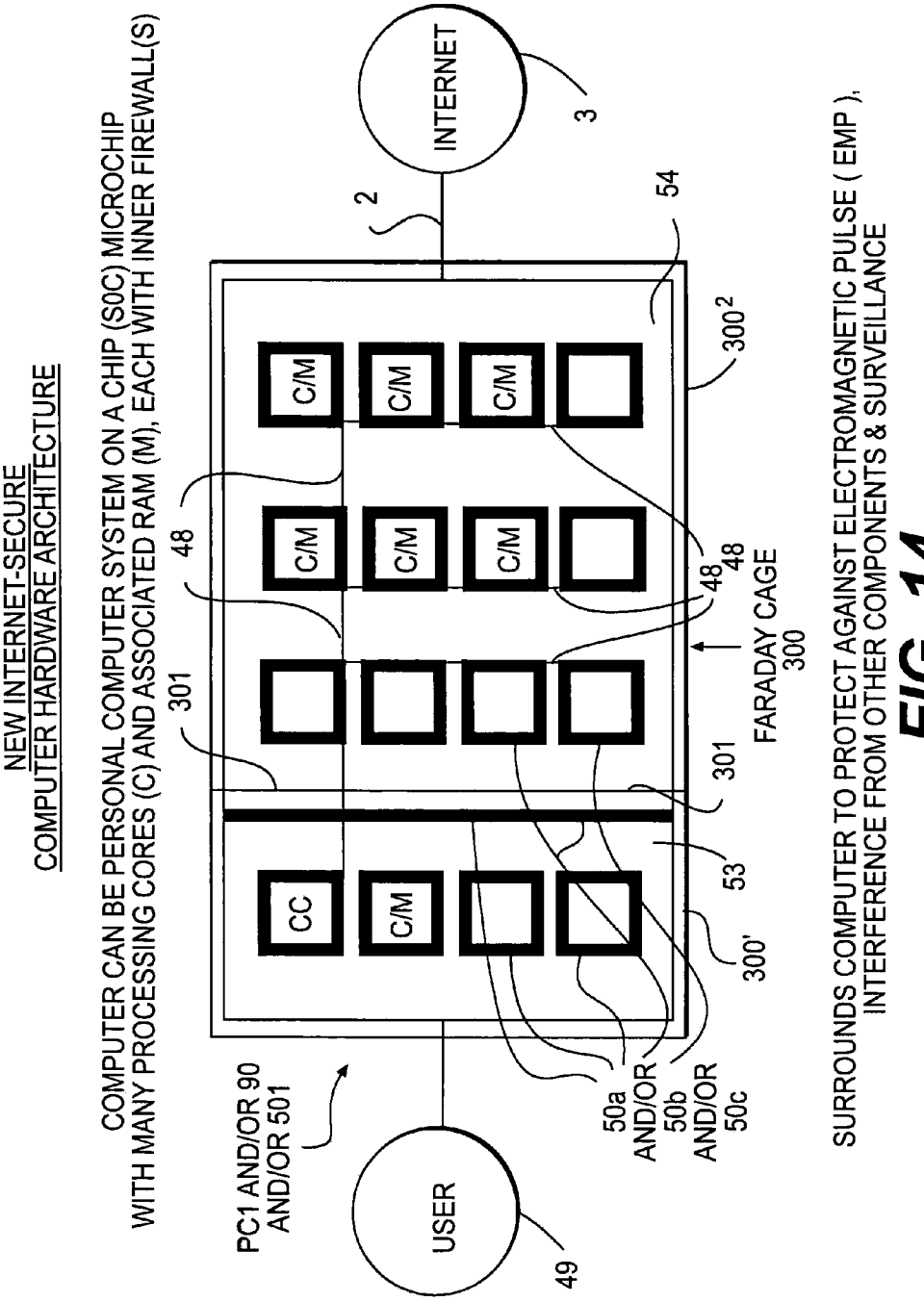

NEW INTERNET-SECURE
COMPUTER HARDWARE ARCHITECTURE
COMPUTER CAN BE PERSONAL COMPUTER SYSTEM ON A CHIP (SOC) MICROCHIP
WITH MANY PROCESSING CORES (C) AND ASSOCIATED RAM (M), EACH WITH INNER FIREWALL(S)
INTERNET
3
2
54
300^2
48
48
48
301
301
FARADAY CAGE
300
CC
C/M
53
300'
PC1 AND/OR 90
AND/OR 501
USER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

FIG. 14

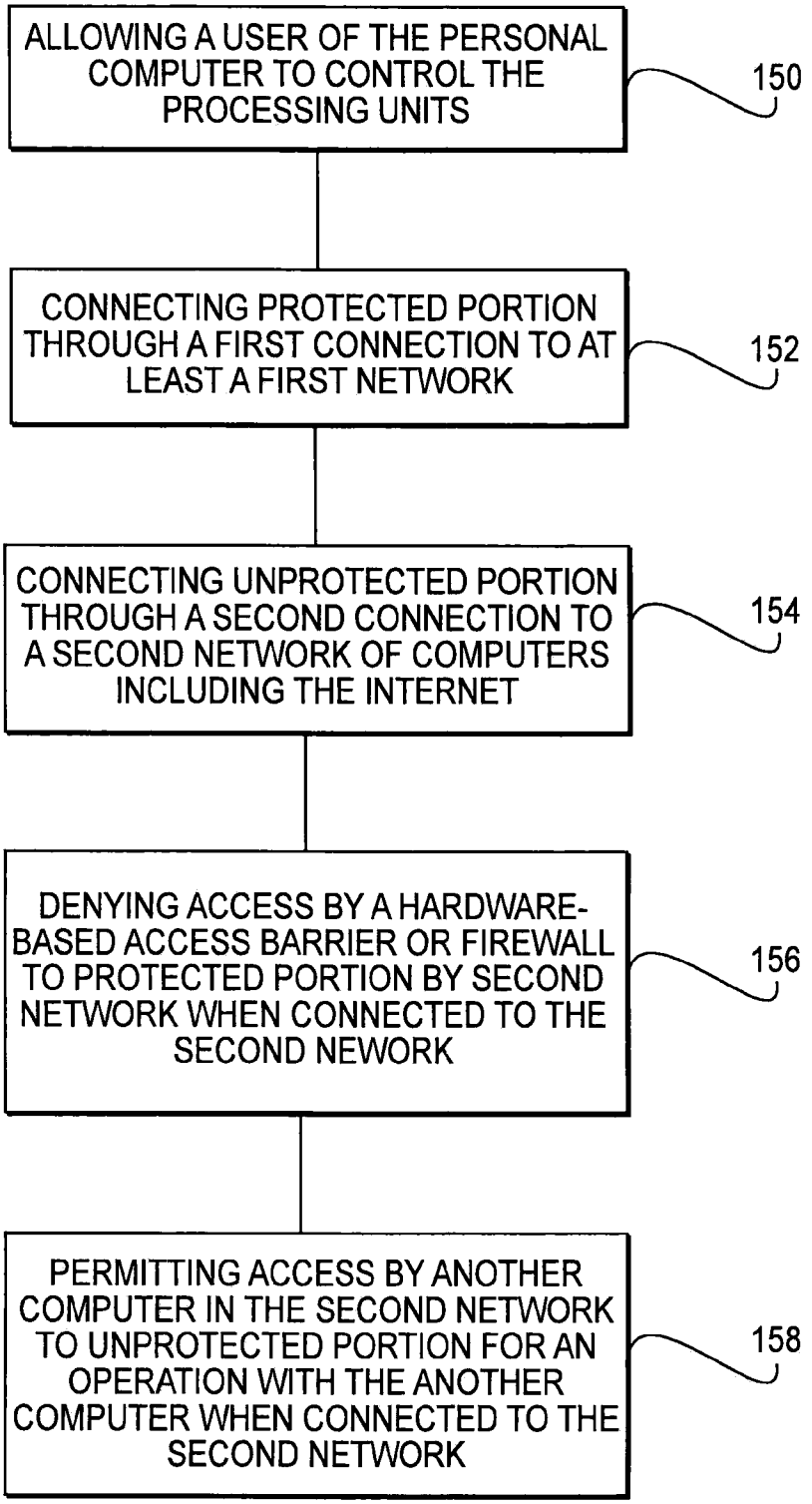

ALLOWING A USER OF THE PERSONAL COMPUTER TO CONTROL THE PROCESSING UNITS
150
CONNECTING PROTECTED PORTION THROUGH A FIRST CONNECTION TO AT LEAST A FIRST NETWORK
152
CONNECTING UNPROTECTED PORTION THROUGH A SECOND CONNECTION TO A SECOND NETWORK OF COMPUTERS INCLUDING THE INTERNET
154
DENYING ACCESS BY 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

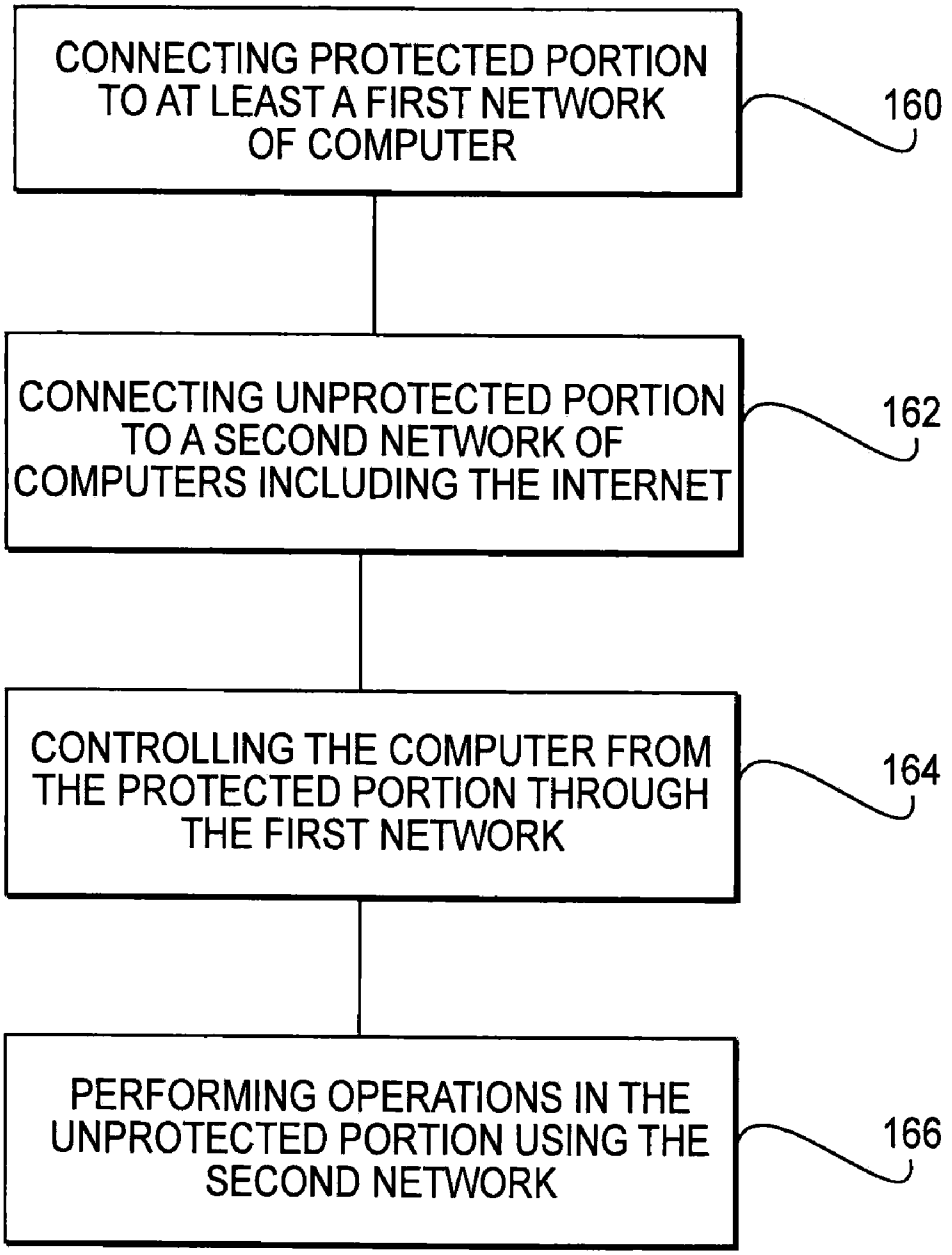

CONNECTING PROTECTED PORTION TO AT LEAST A FIRST NETWORK OF COMPUTER
160
CONNECTING UNPROTECTED PORTION TO A SECOND NETWORK OF COMPUTERS INCLUDING THE INTERNET
162
CONTROLLING THE COMPUTER FROM THE PROTECTED PORTION THROUGH THE FIRST NETWORK
164
PERFORMING OPERATIONS IN THE UNPROTECTED PORTION USING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

FIG. 16

METHOD OF SECURELY CONTROLLING THROUGH ONE OR MORE SEPARATE PRIVATE NETWORKS AN INTERNET-CONNECTED COMPUTER HAVING ONE OR MORE HARDWARE-BASED INNER FIREWALLS OR ACCESS BARRIERS

Applicant claims the right to priority based on U.S. Provisional Patent Application No. 61/282,378, filed Jan. 29, 2010; U.S. Provisional Patent Application No. 61/282,478, filed Feb. 17, 2010; U.S. Provisional Patent Application No. 61/282,503, filed Feb. 22, 2010; U.S. Provisional Patent Application No. 61/282,861, filed Apr. 12, 2010; U.S. Provisional Patent Application No. 61/344,018, filed May 7, 2010; and U.S. Provisional Patent Application No. 61/457,184, filed Jan. 24, 2011.

Applicant also claims the right to priority based on U.S. Nonprovisional patent application Ser. No. 13/014,201, filed Jan. 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 Ser. No. 10/684,657 filed Oct. 15, 2003 and published as Pub. No. US 2005/0180095 A1 on Aug. 18, 2005 and U.S. patent application Ser. No. 12/292,769 filed Nov. 25, 2008 and published as Pub. No. US 2009/0200661 A1 on Aug. 13, 2009.

Also, this application hereby expressly incorporates by reference in its entirety U.S. patent application Ser. No. 10/802,049 filed Mar. 17, 2004 and published as Pub. No. US 2004/0215931 A1 on Oct. 28, 2004 and U.S. patent application Ser. No. 12/292,553 filed Nov. 20, 2008 and published as Pub. No. US 2009/0168329 A1 on Jul. 2, 2009.

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

FIG. **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.

FIG. **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 **50***a*, 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).

FIG. **3** is a similar example embodiment to that shown in FIG. **2**, but with the Private Unit **53** and Public Unit **54** connected by a hardware-based access barrier or firewall **50***b* 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.

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

FIG. **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 **50***c* example that includes the same buses or channels with on/off switches or equivalents as FIG. **4**.

FIG. **6** shows an example embodiment of a personal computer **1** and/or microchip **90** (and/or **501**) similar to FIGS. **23**A and **23**B of the '657 Application, which showed multiple access barriers or firewalls **50** with progressively greater protection, but with hardware-based access barriers or firewalls **50***c*, **50***b*, and **50***a* 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.

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

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

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

FIGS. **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 **50***a*, **50***b*, or **50***c*) 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 PC**1** (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, FIG. **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 (PC**1** 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 (PC**1** 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 **50***a*, **50***b*, or **50***c* 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 (PC**1** and/or **90** and/or **501** and/or **1500**, **1501**, **1502**, or **1503**) linking through wire or wirelessly to his laptop or desktop computer (PC**1** 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 FIG. **6**.

Also shown in FIG. **1** for personal computer PC**1** 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 PC**1** 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 PC**1** and/or microchip **90** and/or **501**, including the Public Unit **54**; the access control barrier or firewall **50** (or **50***a* and/or **50***b* and/or **50***c*) can be removable with the Private Unit **53** or remain with Public Unit **54**.

Similarly, FIG. **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 FIG. **2**, the Private Unit **53** and Public Unit **54** are connected only by an inner hardware-based access barrier or firewall **50***a* 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 FIG. **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 PC**1** 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 PC**1** 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 **50***a* arranged in any configuration.

FIG. **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.

FIG. **3** is a similar useful architectural example embodiment to that shown in FIG. **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 **50***b* 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 authenti-

cated) 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 PC**1** 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 **50***b* arranged in any configuration.

FIG. **4** is a similar useful architectural example embodiment to that shown in FIGS. **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 **50***c* 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 FIG. **17**D 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 PC**1** 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 **50***c* arranged in any configuration.

FIG. **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 **50***c* 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 FIG. **4** example above and can use the same hardwire control. Alternatively, inner hardware-based access barriers or firewalls **50***a* or **50***b* can be used. In addition, inner hardware-based access barriers or firewalls **50***a*, **50***b*, and **50***c* 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 FIGS. **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.

FIG. **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 FIGS. **23**A and **23**B of the '657 Application incorporated by reference above, which showed multiple inner firewalls **50** with progressively greater protection. FIG. **6** shows an example of an internal array of inner hardware-based access barriers or firewalls **50***c*, **50***b*, and **50***a* (described in previous FIGS. **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, FIG. **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 **50***a* and/or **50***b* and/or **50***c* arranged in any combination or configuration.

As shown in FIG. **6**, the private non-Internet network **52**, which was discussed previously relative to FIG. **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 PC**1** 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 PC**1** 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 **50***a* and/or **50***b* and/or **50***c* 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 FIG. **6**.

Also shown in the example embodiment of FIG. **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 FIG. **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). FIG. **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 FIGS. **1-6**, as well as the following FIGS. **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 FIGS. **10**A-**10**D, **10**J-**10**Q, **17**A-**17**D, **23**A-**23**E, **24**, **25**A-**25**D and **27**A-**27**G, and associated textual specification, of the above '657 Application incorporated by reference.

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

FIG. **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.

FIG. **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 FIGS. **10**A-**10**D and **10**J-**10**Q, and associated textual specification of the '657 Application incorporated by reference, as well as earlier in this application. FIG. **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 **50***a* and/or **50***b* and/or **50***c* as described previously in this application; the number and potential configurations of access barriers or firewalls **50***a* and/or **50***b* and/or **50***c* within any computer, such as computer PC**1** and/or microchip **90** (and/or **501**) is without any particular limit.

FIG. **9** is a similar embodiment to FIG. **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). FIG. **8** also shows a computer PC**1** and/or microchip **90** and/or **501** with many microprocessors or cores.

FIG. **10** is the same embodiment as FIG. **9**, but also shows a major functional benefit of the applicant's access barrier or firewall **50***a*, **50***b*, and **50***c* 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 FIGS. **25**A-**25**D and associated textual specification of the '657 Application incorporated by reference earlier.

FIG. **11** is a useful example embodiment similar to FIG. **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 **50***a*, **50***b*, and **50***c*; 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 FIGS. **23**A-**23**B and associated textual specification of the '657 Application incorporated by reference earlier.

FIG. **12** is another useful architectural example embodiment of the layered use of access barriers or firewalls **50**, **50***c*, **50***b*, and **50***c* 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 FIGS. **23**D-**23**E and associated textual specification of the '657 Application incorporated by reference earlier.

FIG. **13** is a useful architectural example embodiment showing the presence of many FIG. **12** layered access barriers or firewalls **50***a*, **50***b*, and **50***c* 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 dis-

cussed in more detail in FIG. **23**C and associated textual specification of the '657 Application incorporated by reference earlier.

FIG. **14** is a useful architectural example embodiment similar to FIG. **13**, but also showing the computer PC**1** 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 FIGS. **27**A-**27**G and associated textual specification of the '657 Application incorporated by reference earlier.

FIG. **14** shows a useful example embodiment of a Faraday Cage **300** surrounding completely a computer PC**1** 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 $\mathbf{300}^1$ and Public Unit **54** is completely surrounded by Faraday Cage $\mathbf{300}^2$, 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 FIG. **14**, including a separate Faraday Cage for any hardware component of the computer or microchip.

The example embodiments shown in FIGS. **1-4**, **6-11**, and **13-16** are a computer of any sort, including a personal computer PC**1**; 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 FIGS. **1-4**, **6-11**, and **13-16**, the computer also including one or more microchips also with the architecture shown in FIGS. **1-4**, **6-11**, and **13-16**.

The Public Unit **54** shown in FIGS. **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 PC**1** 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 $\mathbf{53}^2$, $\mathbf{53}^1$, and **53**.

Privacy in conventional clouds can also be significantly enhanced using the inner hardware-based access barriers or firewalls **50***a* and/or **50***b* and/or **50***c* 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 FIG. **6** shows a computer and/or microchip Public Unit **54** and Private Units **53**, $\mathbf{53}^1$, and $\mathbf{53}^2$, each with a separate Faraday Cage. $\mathbf{300}^4$, $\mathbf{300}^3$, $\mathbf{300}^2$, and $\mathbf{300}^1$, respectively, that are create using partitions $\mathbf{301}^c$, $\mathbf{301}^b$, and $\mathbf{301}^a$, 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.

FIGS. **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 PC**1** 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 FIGS. **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 **50***c* located on the periphery of the computer or microchip to control the connection of the computer PC**1** 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 PC**1** 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 FIGS. **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 fire-

wall 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 FIGS. **1-16** of this application can be usefully combined with one or more features or components of FIGS. **1-31** of the above '657 U.S. Application or FIGS. **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 FIGS. **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 FIGS. **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 FIGS. **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. Pat. Nos. '428, '250, '141, '449, '906, '275, '020, '854, '529, '756, and '233.

The invention claimed is:

1. A method of securely controlling through a private network a computer protected by an inner access barrier or firewall with an out-only bus or channel, said computer being configured to operate as a general purpose computer connected to the Internet, and said computer comprising:

at least one network connection configured for connection to at least a public network of computers including the Internet, said at least one network connection being located in at least one public unit of said computer,

at least one additional and separate private network connection configured for connection to at least a separate, private network of computers, said at least one additional and separate private network connection being located in at least one protected private unit of said computer, and

at least one inner hardware-based access barrier or inner hardware-based firewall that is located between and communicatively connects said at least one protected private unit of said computer and said at least one public unit of said computer;

wherein said private and public units and said two separate network connections are separated by said at least one inner hardware-based access barrier or inner hardware-based firewall; and

wherein said inner hardware-based access barrier or inner hardware-based firewall is configured in a manner such that the at least one protected private unit and the at least one public unit are connected by at least one out-only bus or channel that transmits data and/or code that is output from the at least one protected private unit to be input to the at least one public unit; and

said at least one protected private unit of the computer includes at least a first microprocessor or core or processing unit,

said at least one public unit of the computer includes at least a second microprocessor or core or processing unit, configured to operate as a general purpose microprocessor or core or processing unit, and

said second microprocessor or core or processing unit is separate from said inner hardware-based access barrier or inner hardware-based firewall; and

said method comprising the steps of:

controlling at least one operation of said computer from said private network of computers, said operation including at least transmitting data and/or code from said private network of computers to said separate private network connection in said protected private unit of said computer;

receiving said data and/or code by said first microprocessor or core or processing unit in said protected private unit of said computer; and

transmitting data and/or code by said first microprocessor or core or processing unit in said protected private unit through said out-only bus or channel to at least a part of said public unit.

2. The method of claim **1**, wherein said controlling step includes controlling said computer remotely.

3. The method of claim **1**, wherein said controlling step includes remotely providing administrative functions for said computer.

4. The method of claim 3, wherein said controlling step includes remotely maintaining the computer, remotely testing the computer, or remotely updating an operating or application system of said computer.

5. The method of claim 3, wherein said controlling step includes performing at least one operation in the public unit of said computer.

6. The method of claim 3, wherein said computer further comprises:

at least a separate, second inner hardware-based access barrier or inner hardware-based firewall that protects at least a separate, second private network connection configured for connection to at least a separate, second private network of computers, said at least a second private network connection being located in at least a second protected private unit of said computer;

said second protected private unit of the computer includes at least a third microprocessor or core or processing unit,

said method further comprising the steps of:

controlling at least one operation of said computer from said second private network of computers, said operation including at least transmitting data and/or code from said second private network of computers to said second private network connection in said second protected private unit of said computer; and

receiving said data and/or code in at least a part of said second protected private unit of said computer from said second private network of computers, said part of said second protected private unit including at least said third microprocessor or core or processing unit; and

transmitting data and/or code by said third microprocessor or core or processing unit through said second inner hardware-based access barrier or inner hardware-based firewall to at least a part of said public unit or said protected private unit.

7. The method of claim 6, wherein said computer further comprises:

at least a separate, third inner hardware-based access barrier or inner hardware-based firewall that protects at least a separate, third private network connection configured for connection to at least a separate, third private network of computers, said at least a third private network connection being located in at least a third protected private unit of said computer;

said third protected private unit of the computer includes at least a fourth microprocessor or core or processing unit,

said method further comprising the steps of:

controlling at least one operation of said computer from said third private network of computers, said operation including at least transmitting data and/or code from said third private network of computers to said third private network connection in said third protected private unit of said computer; and

receiving said data and/or code in at least a part of said third protected private unit of said computer from said third private network of computers, said part of said third protected private unit including at least said fourth microprocessor or core or processing unit; and

transmitting data and/or code by said fourth microprocessor or core or processing unit through said third inner hardware-based access bather or inner hardware-based firewall to at least a part of said public unit or said protected private unit or said second protected private unit.

8. A method of securely controlling through a private network a computer protected by an inner access barrier or firewall with an out-only or in-only bus or channel, said computer being configured to operate as a general purpose computer connected to the Internet, and said computer comprising:

at least one network connection configured for connection to at least a public network of computers including the Internet, said at least one network connection being located in at least one public unit of said computer,

at least one additional and separate network connection configured for connection to at least a separate, private network of computers, said at least one additional and separate network connection being located in at least one protected private unit of said computer, and

at least one inner hardware-based access barrier or inner hardware-based firewall that is located between and communicatively connects said at least one protected private unit of said computer and said at least one public unit of said computer; and

wherein said private and public units and said two separate network connections are separated by said at least one inner hardware-based access barrier or inner hardware-based firewall;

wherein said inner hardware-based access barrier or inner hardware-based firewall is configured in a manner such that the at least one protected private unit and the at least one public unit are connected by at least one out-only bus or channel that transmits data and/or code that is output from the at least one protected private unit to be input to the at least one public unit, and said out-only bus or channel includes a hardware output on/off switch;

wherein said inner hardware-based access barrier or inner hardware-based firewall is configured in a manner such that the at least one protected private unit and the at least one public unit are also connected by at least one in-only bus or channel that includes a hardware input on/off switch; and

said at least one protected private unit of the computer includes at least a first microprocessor or core or processing unit,

said at least one public unit of the computer includes at least a second microprocessor or core or processing unit, configured to operate as a general purpose microprocessor or core or processing unit, and

said second microprocessor or core or processing unit is separate from said inner hardware-based access barrier or inner hardware-based firewall; and

said method comprising the steps of:

controlling at least one operation of said computer from said private network of computers, said operation including at least transmitting data and/or code from said private network of computers to said separate private network connection in said protected private unit of said computer;

receiving said data and/or code by said first microprocessor or core or processing unit in said protected private unit of said computer;

transmitting data and/or code by said first microprocessor or core or processing unit in said protected private unit through said out-only bus or channel to at least a part of said public unit; and

receiving data and/or code from said public unit part through said in-only bus or channel to said first microprocessor or core or processing unit.

9. The method of claim 8, wherein said controlling step includes remotely controlling said computer.

10. The method of claim 8, wherein said controlling step includes remotely providing administrative functions for said computer.

11. The method of claim 8, wherein said controlling step includes remotely maintaining the computer, remotely testing the computer, or remotely updating an operating or application system of said computer.

12. The method of claim 8, further comprising the step of performing at least one operation in the public unit of said computer.

13. The method of claim 8, wherein said computer further comprises:

at least a separate, second inner hardware-based access barrier or inner hardware-based firewall that protects at least a separate, second private network connection configured for connection to at least a separate, second private network of computers, said at least a second private network connection being located in at least a second protected private unit of said computer;

said second protected private unit of the computer includes at least a third microprocessor or core or processing unit,

said method further comprising the steps of:

controlling at least one operation of said computer from said second private network of computers, said operation including at least transmitting data and/or code from said second private network of computers to said second private network connection in said second protected private unit of said computer; and

receiving said data and/or code in at least a part of said second protected private unit of said computer from said second private network of computers, said part of said second protected private unit including at least said third microprocessor or core or processing unit; and

transmitting data and/or code by said third microprocessor or core or processing unit through said second inner hardware-based access barrier or inner hardware-based firewall to at least a part of said public unit or said protected private unit.

14. The method of claim 13, wherein said computer further comprises:

at least a separate, third inner hardware-based access barrier or inner hardware-based firewall that protects at least a separate, third private network connection configured for connection to at least a separate, third private network of computers, said at least a third private network connection being located in at least a third protected private unit of said computer;

said third protected private unit of the computer includes at least a fourth microprocessor or core or processing unit,

said method further comprising the steps of:

controlling at least one operation of said computer from said third private network of computers, said operation including at least transmitting data and/or code from said third private network of computers to said third private network connection in said third protected private unit of said computer; and

receiving said data and/or code in at least a part of said third protected private unit of said computer from said third private network of computers, said part of said third protected private unit including at least said fourth microprocessor or core or processing unit; and

transmitting data and/or code by said fourth microprocessor or core or processing unit through said third inner hardware-based access bather or inner hardware-based firewall to at least a part of said public unit or said protected private unit or said second protected private unit.

15. The method of claim 8, wherein said controlling step includes at least said first microprocessor or core or processing unit controlling said hardware output on/off switch and/or said hardware input on/off switch.

16. A method of securely controlling through a second private network a second private unit of a computer protected by an inner access barrier or firewall and configured to operate as a general purpose computer connected to the Internet, said computer comprising:

at least one network connection configured for connection to at least a public network of computers including the Internet, said at least one network connection being located in at least one public unit of said computer,

at least one additional and separate private network connection configured for connection to at least a separate, private network of computers, said at least one additional and separate private network connection being located in at least one protected private unit of said computer, and

at least one inner hardware-based access barrier or inner hardware-based firewall that is located between and communicatively connects said at least one protected private unit of said computer and said at least one public unit of said computer;

wherein said private and public units and said two separate network connections are separated by said at least one inner hardware-based access barrier or inner hardware-based firewall; and

said at least one protected private unit of the computer includes at least a first microprocessor or core or processing unit,

said at least one public unit of the computer includes at least a second microprocessor or core or processing unit, configured to operate as a general purpose microprocessor or core or processing unit, and

said second microprocessor or core or processing unit is separate from said inner hardware-based access barrier or inner hardware-based firewall; and

at least a separate, second inner hardware-based access barrier or inner hardware-based firewall that protects at least a separate, second private network connection configured for connection to at least a separate, second private network of computers, said at least a second private network connection being located in at least a second protected private unit of said computer;

said second protected private unit of the computer includes at least a third microprocessor or core or processing unit,

said method comprising the steps of:

controlling at least one operation of said computer from said second private network of computers, said operation including at least transmitting data and/or code from said second private network of computers to said second private network connection in said second protected private unit of said computer; and

receiving said data and/or code in at least a part of said second protected private unit of said computer from said second private network of computers, said part of said second protected private unit including at least said third microprocessor or core or processing unit; and

transmitting data and/or code by said third microprocessor or core or processing unit through said second inner

hardware-based access barrier or inner hardware-based firewall to at least a part of said public unit or said protected private unit.

17. The method of claim **16**, wherein said controlling step includes remotely controlling said second private protected unit of said computer.

18. The method of claim **16**, wherein said controlling step includes remotely providing administrative functions for said second private protected unit of said computer.

19. The method of claim **16**, wherein said controlling step includes remotely maintaining the second private protected unit of said computer, remotely testing the second private protected unit of said computer, or remotely updating an operating or application system of said second private protected unit of said computer.

20. The method of claim **16**, further comprising the step of performing at least one operation in the public unit of said computer.

21. A method of securely controlling through a third private network a third private unit of a computer protected by an inner access barrier or firewall and configured to operate as a general purpose computer connected to the Internet, said computer comprising:

at least one network connection configured for connection to at least a public network of computers including the Internet, said at least one network connection being located in at least one public unit of said computer,

at least one additional and separate network connection configured for connection to at least a separate, private network of computers, said at least one additional and separate network connection being located in at least one protected private unit of said computer, and

at least one inner hardware-based access barrier or inner hardware-based firewall that is located between and communicatively connects said at least one protected private unit of said computer and said at least one public unit of said computer; and

wherein said private and public units and said two separate network connections are separated by said at least one inner hardware-based access barrier or inner hardware-based firewall; and

said at least one protected private unit of the computer includes at least a first microprocessor or core or processing unit,

said at least one public unit of the computer includes at least a second microprocessor or core or processing unit, configured to operate as a general purpose microprocessor or core or processing unit, and

said second microprocessor or core or processing unit is separate from said inner hardware-based access barrier or inner hardware-based firewall; and

at least a separate, second inner hardware-based access barrier or inner hardware-based firewall that protects at least a separate, second private network connection configured for connection to at least a separate, second private network of computers, said at least a second private network connection being located in at least a second protected private unit of said computer;

said second protected private unit of the computer includes at least a third microprocessor or core or processing unit,

at least a separate, third inner hardware-based access barrier or inner hardware-based firewall that protects at least a separate, third private network connection configured for connection to at least a separate, third private network of computers, said at least a third private network connection being located in at least a third protected private unit of said computer;

said third protected private unit of the computer includes at least a fourth microprocessor or core or processing unit,

said method comprising the steps of:

controlling at least one operation of said computer from said third private network of computers, said operation including at least transmitting data and/or code from said third private network of computers to said third private network connection in said third protected private unit of said computer; and

receiving said data and/or code in at least a part of said third protected private unit of said computer from said third private network of computers, said part of said third protected private unit including at least said fourth microprocessor or core or processing unit; and

transmitting data and/or code by said fourth microprocessor or core or processing unit through said third inner hardware-based access bather or inner hardware-based firewall to at least a part of said public unit or said protected private unit or said second protected private unit.

22. The method of claim **21**, wherein said controlling step includes remotely controlling said third private protected unit of said computer.

23. The method of claim **21**, wherein said controlling step includes remotely providing administrative functions for said third private protected unit of said computer.

24. The method of claim **21**, wherein said controlling step includes remotely maintaining the third private protected unit of said computer, remotely testing the third private protected unit of said computer, or remotely updating an operating or application system of said third private protected unit of said computer.

25. The method of claim **21**, further comprising the step of performing at least one operation in the public unit of said computer.

26. A method of securely controlling through a private network a computer protected by an inner access barrier or firewall, configured for connection to the Internet, said computer comprising:

at least one network connection configured for connection to at least a public network of computers including the Internet, said at least one network connection being located in at least one public unit of said computer,

at least one additional and separate private network connection configured for connection to at least a separate, private network of computers, said at least one additional and separate private network connection being located in at least one protected private unit of said computer, and

at least one inner hardware-based access barrier or inner hardware-based firewall that is located between and communicatively connects said at least one protected private unit of said computer and said at least one public unit of said computer;

wherein said private and public units and said two separate network connections are separated by said at least one inner hardware-based access barrier or inner hardware-based firewall; and

wherein said inner hardware-based access barrier or inner hardware-based firewall is configured in a manner such that the at least one protected private unit and the at least one public unit are connected by at least an out-only bus or channel that transmits data and/or

code that is output from the at least one protected private unit to be input to the at least one public unit; and

said at least one protected private unit of the computer includes at least a first microprocessor or core or processing unit,

said at least one public unit of the computer includes at least a second microprocessor or core or processing unit, and

said second microprocessor or core or processing unit is separate from said inner hardware-based access barrier or inner hardware-based firewall; and

said method comprising the steps of:

controlling at least one operation of said computer from said private network of computers, said operation including at least transmitting data and/or code from said private network of computers to said separate private network connection in said protected private unit of said computer;

receiving said data and/or code by said first microprocessor or core or processing unit in said protected private unit of said computer; and

transmitting data and/or code by said first microprocessor or core or processing unit in said protected private unit through said out-only bus or channel to at least a part of said public unit.

27. The method of claim **26**, wherein:

said out-only bus or channel also includes a hardware output on/off switch, and

said inner hardware-based access barrier or inner hardware-based firewall is configured in a manner such that the at least one protected private unit and the at least one public unit are also connected by an in-only bus or channel that includes a hardware input on/off switch; and

said method further comprising the step of:

receiving data and/or code from said public unit part through said in-only bus or channel to said first microprocessor or core or processing unit.

28. A method of securely controlling through a second private network a second private unit of a computer protected by an inner access barrier or firewall, configured for connection to the Internet, said computer comprising:

at least one network connection configured for connection to at least a public network of computers including the Internet, said at least one network connection being located in at least one public unit of said computer,

at least one additional and separate private network connection configured for connection to at least a separate, private network of computers, said at least one additional and separate private network connection being located in at least one protected private unit of said computer, and

at least one inner hardware-based access barrier or inner hardware-based firewall that is located between and communicatively connects said at least one protected private unit of said computer and said at least one public unit of said computer;

wherein said private and public units and said two separate network connections are separated by said at least one inner hardware-based access barrier or inner hardware-based firewall; and

said at least one protected private unit of the computer includes at least a first microprocessor or core or processing unit,

said at least one public unit of the computer includes at least a second microprocessor or core or processing unit, and

said second microprocessor or core or processing unit is separate from said inner hardware-based access barrier or inner hardware-based firewall; and

at least a separate, second inner hardware-based access barrier or inner hardware-based firewall that protects at least a separate, second private network connection configured for connection to at least a separate, second private network of computers, said at least a second private network connection being located in at least a second protected private unit of said computer;

said second protected private unit of the computer includes at least a third microprocessor or core or processing unit,

said method comprising the steps of:

controlling at least one operation of said computer from said second private network of computers, said operation including at least transmitting data and/or code from said second private network of computers to said second private network connection in said second protected private unit of said computer; and

receiving said data and/or code in at least a part of said second protected private unit of said computer from said second private network of computers, said part of said second protected private unit including at least said third microprocessor or core or processing unit; and

transmitting data and/or code by said third microprocessor or core or processing unit through said second inner hardware-based access barrier or inner hardware-based firewall to at least a part of said public unit or said protected private unit.

29. The method of claim **28**, wherein said computer further comprises:

at least a separate, third inner hardware-based access barrier or inner hardware-based firewall that protects at least a separate, third private network connection configured for connection to at least a separate, third private network of computers, said at least a third private network connection being located in at least a third protected private unit of said computer;

said third protected private unit of the computer includes at least a fourth microprocessor or core or processing unit,

said method further comprising the steps of:

controlling at least one operation of said computer from said third private network of computers, said operation including at least transmitting data and/or code from said third private network of computers to said third private network connection in said third protected private unit of said computer; and

receiving said data and/or code in at least a part of said third protected private unit of said computer from said third private network of computers, said part of said third protected private unit including at least said fourth microprocessor or core or processing unit; and

transmitting data and/or code by said fourth microprocessor or core or processing unit through said third inner hardware-based access bather or inner hardware-based firewall to at least a part of said public unit or said protected private unit or said second protected private unit.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO.	: 8,171,537 B2
APPLICATION NO.	: 13/016527
DATED	: May 1, 2012
INVENTOR(S)	: Frampton E. Ellis

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Claim 7, col. 15, line 64, "bather" should read --barrier--.

Signed and Sealed this
Seventh Day of August, 2012

David J. Kappos

David J. Kappos
Director of the United States Patent and Trademark Office