UNITED STATES DISTRICT COURT
DISTRICT OF DELAWARE

STRIKEFORCE TECHNOLOGIES, INC.,
1090 King Georges Post Road
Edison, New Jersey 08837,

Plaintiff,

v.

PHONEFACTOR, INC.
7301 West 129th Street
Overland Park, Kansas 66213,

And

FISERV, INC.
255 Fiserv Drive
Brookfield, Wisconsin 53045,

And

FIRST MIDWEST BANCORP, INC.
One Pierce Place, Suite 1500
Itasca, Illinois 60143-9768,

Defendants.

Case No.

COMPLAINT FOR PATENT INFRINGEMENT

Jury Trial Demanded

StrikeForce Technologies, Inc. (hereinafter "Plaintiff"), files this Complaint for patent infringement against PhoneFactor, FiServ, Inc., and First Midwest Bancorp, Inc., (hereinafter "Defendants"), and, in support thereof, further states and alleges as follows:

THE PARTIES

1. Plaintiff, StrikeForce Technologies, Inc. is a corporation incorporated in the state of Wyoming, with its principal place of business located at 1090 King Georges Post Road, Edison, New Jersey 08837.

2. Upon information and belief, Defendant PhoneFactor, Inc. is a corporation incorporated in the state of Delaware, having its principal place of business at 7301 West 129th Street, Overland Park, Kansas 66213. The registered agent for process of service is Corporation

Service Company located at 2711 Centerville Road, Suite 400, Wilmington, DE 19808.

3. Upon information and belief, Defendant Fiserv, Inc. is a corporation incorporated in the state of Delaware, with its principal place of business at 255 Fiserv Drive, Brookfield, Wisconsin 53045. The registered agent for process of service is The Corporation Trust Company located at Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801.

4. Upon information and belief, Defendant First Midwest Bancorp, Inc., is a corporation incorporated in the state of Delaware, with its principal place of business at One Pierce Place, Suite 1500, Itasca, Illinois 60143-9768. The registered agent for process of service is United States Corporation Company, 2711 Centerville Road, Suite 400, Wilmington, DE 19808. On further information and belief, Defendant First Midwest Bancorp, conducts banking operations in the name of First Midwest Bank.

JURISDICTION AND VENUE

5. This is a civil action for patent infringement under the laws of the United States, Title 35 United States Code §§ 1, *et seq.*

6. This Court has subject-matter jurisdiction over this action under 28 U.S.C. §§ 1331 (federal question) and 1338(a) (patent-exclusive jurisdiction).

7. This Court has personal jurisdiction over Defendants because the Defendants are incorporated in the state of Delaware.

8. Venue is proper under 28 U.S.C. §§ 1391(b) and (c) and § 1400(b), because Defendants are subject to personal jurisdiction in this judicial district.

FACTUAL BACKGROUND

9. On January 11, 2011, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 7,870,599, entitled "Multichannel Device Utilizing a Centralized Out-of-Band Authentication System (COBAS)" ("the '599 Patent").

On December 27, 2011, the United States Patent and Trademark Office duly and legally issued Ex Parte Reexamination Certificate No. 7,870,599C1. A true and correct copy of the '599 Patent, including the '599C1 Certificate, is attached hereto as Exhibit A.

10. Plaintiff, StrikeForce Technologies, Inc. is the owner by assignment of the '599 Patent.

11. The'599 Patent is directed to a multichannel security system and method for authenticating a user seeking to gain access to, for example, Internet websites and VPN networks, such as those used for conducting banking, social networking, business activities, and other online services. Such technology is sometimes known as "out-of-band" authentication.

12. StrikeForce offers a product having out-of-band authentication, known as ProtectID®. Since at least as early as February 10, 2011, the statutory notice was placed on the ProtectID® product.

13. On or about February 26, 2009, Defendant PhoneFactor submitted to the U.S. Patent and Trademark Office application no. 12/394,016, which included claims directed to out-of-band authentication.

14. On May 2, 2011, StrikeForce Technologies' counsel sent a letter to Defendant PhoneFactor's counsel giving him actual notice of the '599 Patent.

15. On October 10, 2012, StrikeForce Technologies' counsel sent a letter to Defendant PhoneFactor's Chief Executive Officer counsel giving him actual notice of the '599 Patent.

16. Neither PhoneFactor nor its counsel has responded to either of those letters.

COUNT I

Direct Infringement of the '599 Patent

17. Plaintiff incorporates by this reference the averments set forth in paragraphs 1

through 16.

18. Upon information and belief, each Defendant has infringed the '599 Patent in this district and elsewhere by making, using, offering for sale, or selling a system and method for out-of-band authentication.

19. Upon information and belief, since before the filing of this lawsuit, Defendant PhoneFactor has had actual or constructive knowledge of the '599 Patent at least through its filing and prosecuting the '016 application.

20. Since before the filing of this lawsuit, Defendant PhoneFactor has had actual notice of the'599 Patent by virtue of the letters sent by StrikeForce's counsel to PhoneFactor and its counsel in May 2011 and October 2012.

21. As a direct and proximate result of Defendants' acts of infringing the '599 Patent, Plaintiff has suffered injury and monetary damages for which Plaintiff is entitled to relief in the form of damages for lost profits and in no event less than a reasonable royalty to compensate for Defendants' infringement.

22. Upon information and belief, Defendants have knowingly, willfully, and deliberately infringed the '599 Patent in conscious disregard of Plaintiff's rights, making this case exceptional within the meaning of 35 U.S.C. § 285 and justifying treble damages pursuant to 35 U.S.C. § 284.

23. Upon information and belief, Defendants will continue to directly infringe the '599 Patent, causing immediate and irreparable harm to Plaintiff unless this Court enjoins and restrains Defendants' activities, specifically the acts of making, using, selling, offering for sale, and importing as mentioned above.

24. Upon information and belief, the direct infringement of the '599 Patent by Defendants has deprived, and will deprive, Plaintiff of sales proceeds, subscription fees, licensing fees, royalties and other related revenue which Plaintiff would have made or would enjoy in the future; has injured Plaintiff in other respects; and will cause Plaintiff added injury and damage unless Defendants are enjoined from infringing the '599 Patent on all products and web services Defendants will make, use, offer for sale, sell, import, distribute, market, or advertise until the expiration of the '599 Patent.

COUNT II

Active Inducement of Infringement of the '599 Patent

25. Plaintiff incorporates by this reference the averments contained in paragraphs 1 through 24.

26. Upon information and belief, Defendants have under 35 U.S.C. § 271(b), indirectly infringed, and continue to indirectly infringe the '599 Patent by, *inter alia*, inducing others to make, use, sell, offer for sale, and/or import into the United States the above-mentioned products and services covered by the '599 Patent, and distributing, marketing, and/or advertising those products and web services covered by the '599 Patent in this judicial district and elsewhere in the United States.

27. The customers of Defendants directly infringe the claims of '599 Patent by, for example, placing every element of the claimed systems into use, having control over those systems when used, and directly benefiting from the use of those systems.

28. Upon information and belief, Defendants are also aware that they provide their customers with products and web services that are used in a manner that infringes the '599 Patent.

29. Upon information and belief, Defendants know that their customers are using Defendants' products and web services in an infringing manner.

30. Upon information and belief, Defendants specifically encourage and instruct their customers to use Defendants' products and web services in a manner that infringes the '599 Patent.

31. The Defendants and their customers combine to perform all of the steps of the claims of the '599 Patent, thus subjecting the Defendants to liability for indirect infringement.

32. As a direct and proximate result of Defendants' acts of infringing the '599 Patent, Plaintiff has suffered injury and monetary damages for which Plaintiff is entitled to relief in the form of damages for lost profits and in no event less than a reasonable royalty to compensate for Defendants' infringement.

33. Upon information and belief, Defendants have knowingly, willfully, and deliberately induced infringement of the '599 Patent in conscious disregard of Plaintiff's rights, making this case exceptional within the meaning of 35 U.S.C. § 285 and justifying treble damages pursuant to 35 U.S.C. § 284.

34. Upon information and belief, Defendants will continue to induce infringement of the '599 Patent, causing immediate and irreparable harm to Plaintiff unless this Court enjoins and restrains Defendants' activities, specifically the acts of making, using, selling, offering for sale, and importing as mentioned above.

35. Upon information and belief, the induced infringement of the '599 Patent by Defendants has, and will, deprive Plaintiff of sales, licensing fees, royalties and other related revenue which Plaintiff would have made or would enjoy in the future; has injured Plaintiff in other respects; and will cause Plaintiff added injury and damage unless Defendants

are enjoined from inducing infringement of the '599 Patent on all products and web services Defendants will make, use, offer for sale, sell, import, distribute, market, or advertise until the expiration of the '599 Patent.

COUNT III
Contributory Infringement of the '599 Patent

36. StrikeForce incorporates by this reference the averments set forth in paragraphs 1 through 35.

37. Upon information and belief, Defendants have under 35 U.S.C. § 271(c), indirectly infringed, and continue to indirectly infringe the '599 Patent by, *inter alia*, providing to their customers a material component of the system that was especially made or adapted for use in that system, which is not a staple article or commodity of commerce and which has no substantial, non-infringing use.

38. The Defendants had and have knowledge of the '599 Patent.

39. As a direct and proximate result of Defendants' acts of infringing the '599 Patent, Plaintiff has suffered injury and monetary damages for which Plaintiff is entitled to relief in the form of damages for lost profits and in no event less than a reasonable royalty to compensate for Defendants' infringement.

40. Upon information and belief, Defendants have knowingly, willfully, and deliberately contributed to infringement of the '599 Patent in conscious disregard of Plaintiff's rights, making this case exceptional within the meaning of 35 U.S.C. § 285 and justifying treble damages pursuant to 35 U.S.C. § 284.

41. Upon information and belief, Defendants will continue to contribute to infringement of the '599 Patent, causing immediate and irreparable harm to Plaintiff unless this Court enjoins and restrains Defendants' activities, specifically the acts of making, using,

selling, offering for sale, and importing as mentioned above.

42. Upon information and belief, the contributory infringement of the '599 Patent by Defendants has, and will, deprive Plaintiff of sales, licensing fees, royalties and other related revenue which Plaintiff would have made or would enjoy in the future; has injured Plaintiff in other respects; and will cause Plaintiff added injury and damage unless Defendants are enjoined from inducing infringement of the '599 Patent on all products and web services Defendants will make, use, offer for sale, sell, import, distribute, market, or advertise until the expiration of the '599 Patent.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, StrikeForce Technologies, Inc., respectfully requests this Court to:

A. Enter judgment for Plaintiff that the '599 Patent was duly and legally issued, is valid, enforceable, and has been infringed, directly or indirectly, by Defendants;

B. Enter judgment for Plaintiff that Defendants have willfully infringed, and are willfully infringing, one or more claims of the '599 Patent;

C. Order Defendants to account in written form for and to pay to Plaintiff actual damages to compensate Plaintiff for Defendants' infringement of the '599 Patent through and including the date of entry of the judgment on the jury's verdict, including but not limited to, damages for lost profits and in no event less than a reasonable royalty, together with interest and costs under 35 U.S.C. § 284.

D. Award Plaintiff treble damages due to Defendants' deliberate, willful, and knowing conduct;

E. Issue a preliminary injunction restraining the Defendants, their directors, officers, agents, employees, successors, subsidiaries, assigns, affiliates and all persons acting in privity or

in concert or participation with any of them from the continued infringement, direct or contributory, or active inducement of infringement by others, of the '599 Patent;

F. Issue a permanent injunction restraining the Defendants, their directors, officers, agents, employees, successors, subsidiaries, assigns, affiliates and all persons acting in privity or in concert or participation with any of them from the continued infringement, direct or contributory, or active inducement of infringement by others, of the '599 Patent;

G. Direct Defendants to file with this Court, and to serve on Plaintiff, a written report under oath setting forth in detail the manner and form in which Defendants have complied with the injunction;

H. In lieu of a permanent injunction, order the Defendants to pay to Plaintiff monetary damages that will be suffered as a result of Defendants' continuing post-verdict infringement of the '599 Patent by requiring the Defendants to take a compulsory license at a reasonable royalty rate to be determined by the Court on all products that Defendants make, use, offer for sale, sell, import, distribute, market, or advertise that infringe the '599 Patent until the expiration of the '599 Patent, which royalty payments shall commence three months after entry of the judgment and shall be made quarterly thereafter, and shall be accompanied by an accounting of the sales of infringing products by the Defendants;

I. Order such other measures in the form of audit rights, interest on late payments, and appropriate security to protect Plaintiff's rights;

J. Order Defendants to pay Plaintiff its costs, expenses, and fees, including reasonable attorneys' fees pursuant to 35 U.S.C. § 285, and pre-judgment and post-judgment interest at the maximum rate allowed by law; and

K. Grant Plaintiff such other and further relief as the Court may deem just and proper.

JURY DEMAND

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiff demands that the issues in this case be tried by a jury.

Dated: March 28, 2013

/s/Steven L. Caponi
Steven L. Caponi (DE No. 3484)
BLANK ROME LLP
1201 Market Street, Suite 800
Wilmington, Delaware 19801
Telephone: (302) 425-6408
Facsimile: (302) 428-5106
E-mail: Caponi@BlankRome.com

ATTORNEY FOR PLAINTIFF
STRIKEFORCE TECHNOLOGIES, INC.

OF COUNSEL FOR PLAINTIFF
STRIKEFORCE TECHNOLOGIES, INC.

Paul M. Honigberg
Peter S. Weissman
BLANK ROME LLP
600 New Hampshire Avenue, N.W.
Suite 1200
Washington, DC 20037
Telephone: (202) 772-5800
Facsimile: (202) 772-5858
E-mail: Honigberg@BlankRome.com
E-mail: Weissman@BlankRome.com

EXHIBIT A

(12) **United States Patent**
Pemmaraju

(10) **Patent No.: US 7,870,599 B2**
(45) **Date of Patent: Jan. 11, 2011**

(54) **MULTICHANNEL DEVICE UTILIZING A CENTRALIZED OUT-OF-BAND AUTHENTICATION SYSTEM (COBAS)**

(75) Inventor: **Ram Pemmaraju**, Old Bridge, NJ (US)

(73) Assignee: **Netlabs.com, Inc.**, Edison, NJ (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 757 days.

(21) Appl. No.: **10/970,559**

(22) Filed: **Oct. 21, 2004**

(65) **Prior Publication Data**

US 2006/0041755 A1 Feb. 23, 2006

Related U.S. Application Data

(63) Continuation-in-part of application No. 09/655,297, filed on Sep. 5, 2000, now abandoned.

(51) **Int. Cl.**
G06F 7/04 (2006.01)
G06F 21/00 (2006.01)
H04L 29/06 (2006.01)

(52) **U.S. Cl.** **726/2**; 726/4; 713/186; 713/168; 713/169; 340/5.8; 340/5.81; 340/5.82; 340/5.83; 340/5.84

(58) **Field of Classification Search** 726/2, 726/5; 713/186, 168 170; 340/8.5 5.84
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,153,918 A * 10/1992 Tuni 713/182
5,915,001 A * 6/1999 Uppaluru 379/88.22
6,012,144 A * 1/2000 Pickett 726/26
6,088,431 A * 7/2000 LaDue 379/114.2
6,088,683 A * 7/2000 Jalili 705/26
6,219,793 B1 * 4/2001 Li et al. 726/19
6,934,858 B2 * 8/2005 Woodhill 726/5
2004/0030935 A1 * 2/2004 Kai 713/202

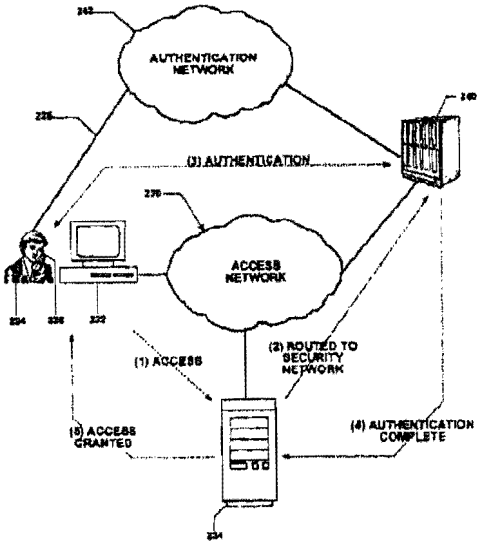
* cited by examiner

Primary Examiner—Kambiz Zand
Assistant Examiner—William S Powers
(74) *Attorney, Agent, or Firm* Blank Rome LLP

(57) **ABSTRACT**

A multichannel security system is disclosed, which system is for granting and denying access to a host computer in response to a demand from an access-seeking individual and computer. The access-seeker has a peripheral device operative within an authentication channel to communicate with the security system. The access-seeker initially presents identification and password data over an access channel which is intercepted and transmitted to the security computer. The security computer then communicates with the access-seeker. A biometric analyzer—a voice or fingerprint recognition device—operates upon instructions from the authentication program to analyze the monitored parameter of the individual. In the security computer, a comparator matches the biometric sample with stored data, and, upon obtaining a match, provides authentication. The security computer instructs the host computer to grant access and communicates the same to the access-seeker, whereupon access is initiated over the access channel.

34 Claims, 18 Drawing Sheets



PRIOR ART

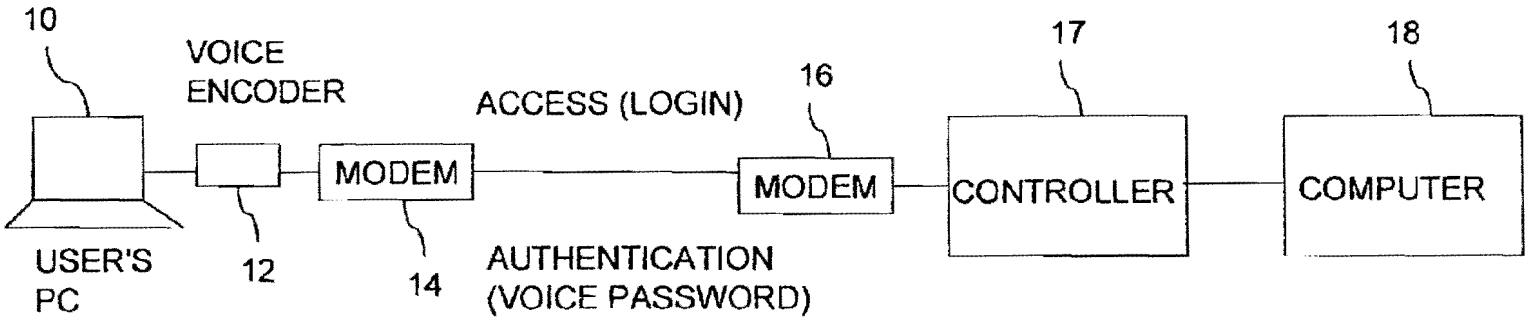


FIGURE 1

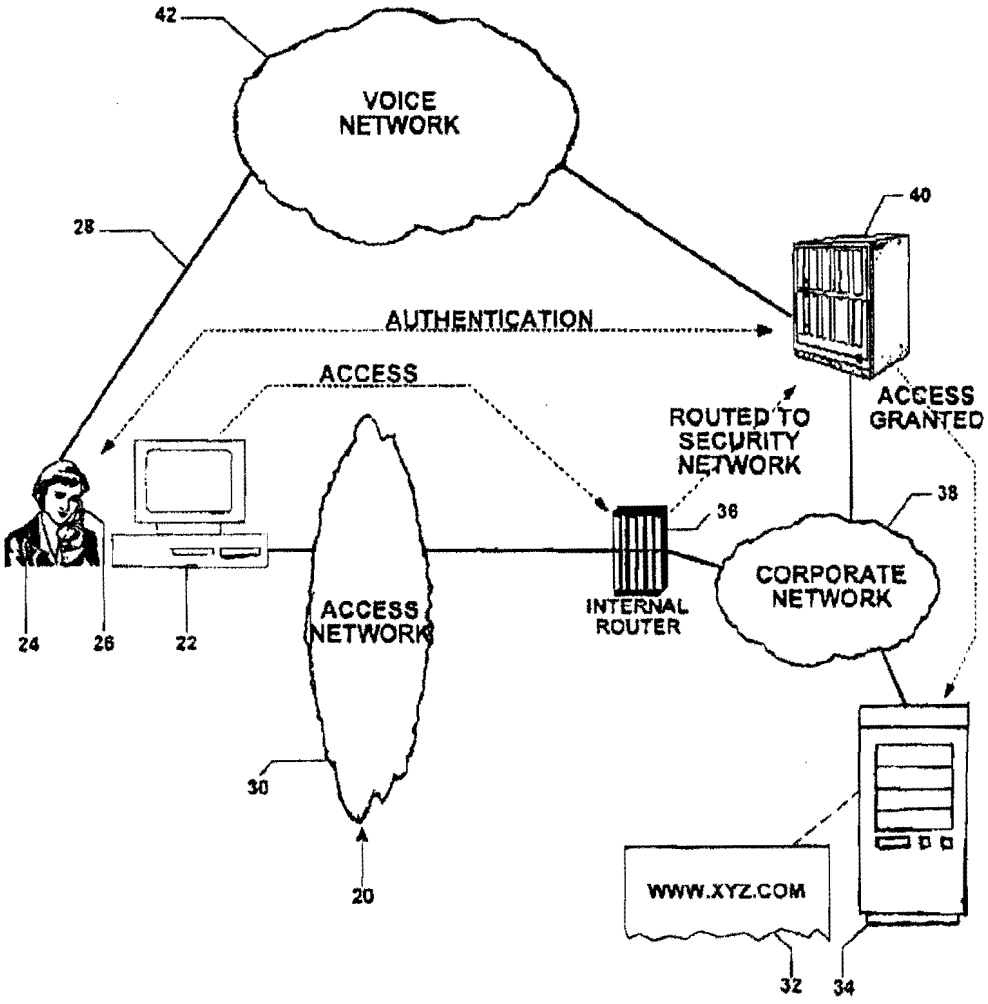

42
VOICE NETWORK
28
40
AUTHENTICATION
ACCESS
ROUTED TO SECURITY NETWORK
ACCESS GRANTED
36
38
CORPORATE NETWORK
INTERNAL ROUTER
ACCESS NETWORK
24
26
22
30
20
WWW.XYZ.COM
32
34

FIGURE 1A

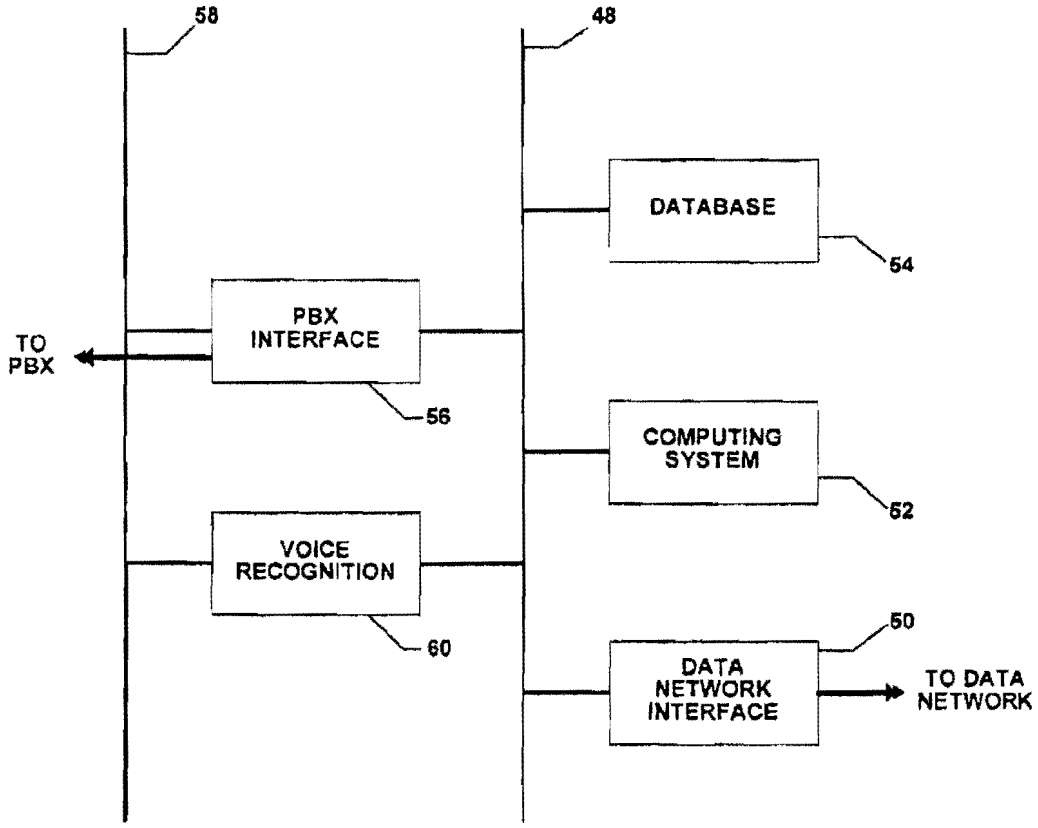

58
48
DATABASE
54
PBX
INTERFACE
TO
PBX
56
COMPUTING
SYSTEM
52
VOICE
RECOGNITION
60
50
DATA
NETWORK
INTERFACE
TO DATA
NETWORK

FIGURE 2

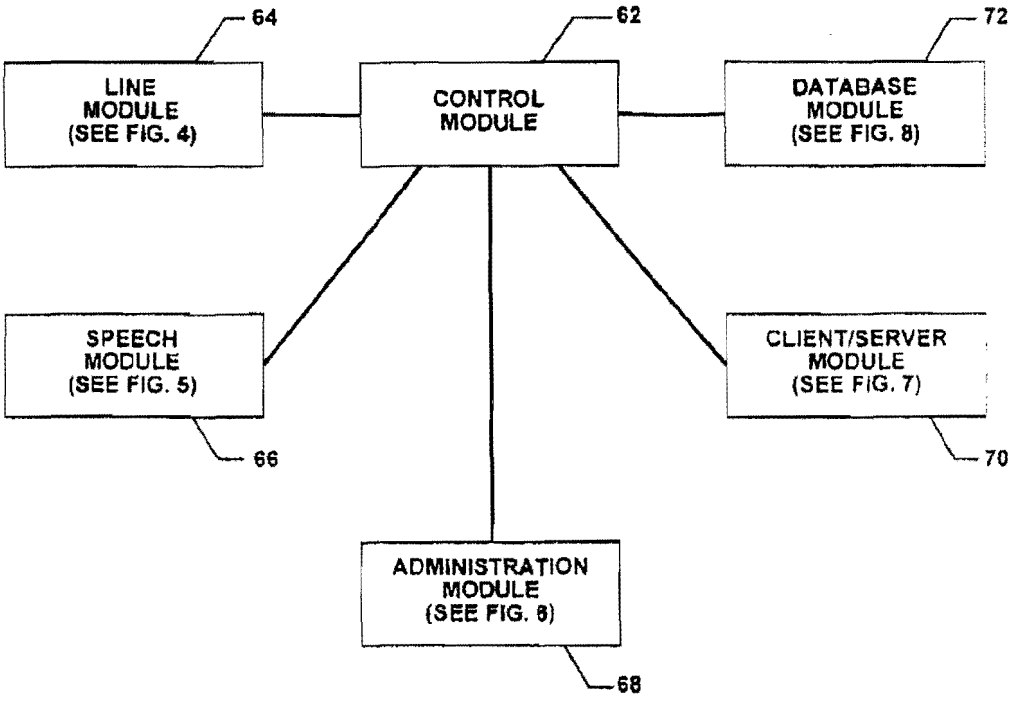

64
62
72
LINE MODULE (SEE FIG. 4)
CONTROL MODULE
DATABASE MODULE (SEE FIG. 8)
SPEECH MODULE (SEE FIG. 5)
CLIENT/SERVER MODULE (SEE FIG. 7)
66
70
ADMINISTRATION MODULE (SEE FIG. 6)
68

FIGURE 3

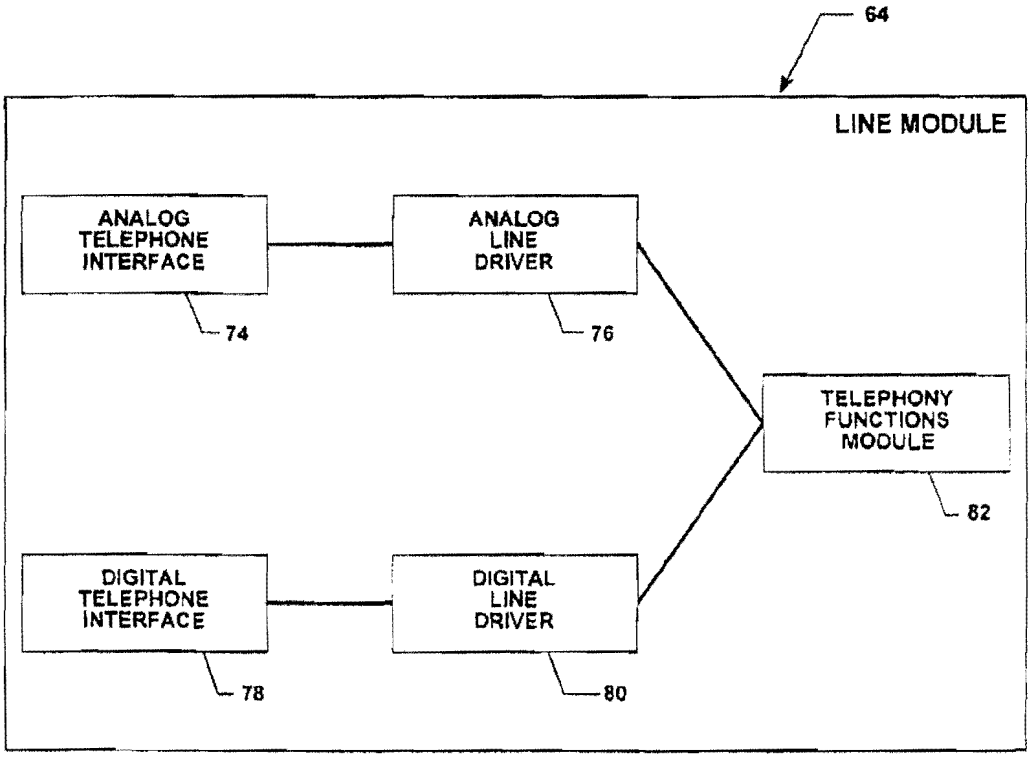

64
LINE MODULE
ANALOG TELEPHONE INTERFACE
74
ANALOG LINE DRIVER
76
TELEPHONY FUNCTIONS MODULE
82
DIGITAL TELEPHONE INTERFACE
78
DIGITAL LINE DRIVER
80

FIGURE 4

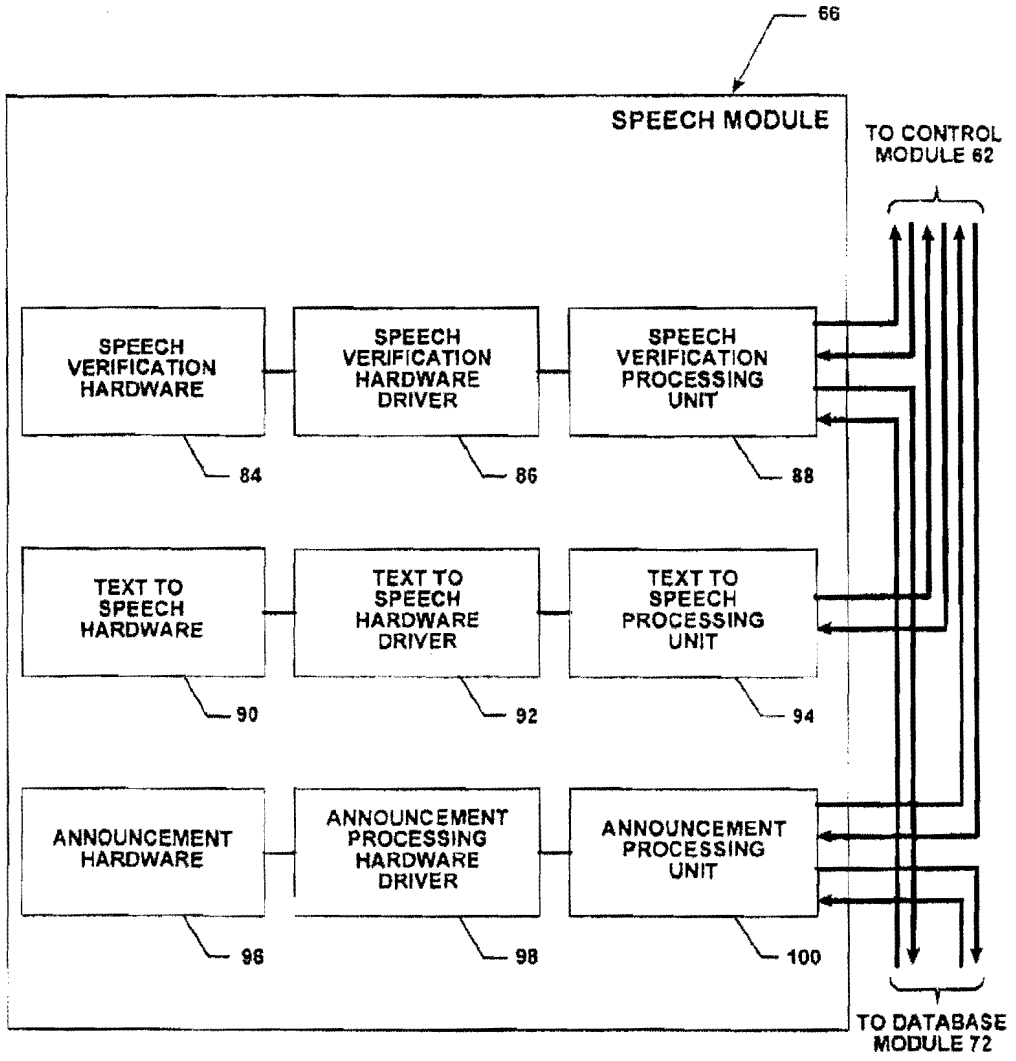

66
SPEECH MODULE
TO CONTROL MODULE 62
SPEECH VERIFICATION HARDWARE
SPEECH VERIFICATION HARDWARE DRIVER
SPEECH VERIFICATION PROCESSING UNIT
84
86
88
TEXT TO SPEECH HARDWARE
TEXT TO SPEECH HARDWARE DRIVER
TEXT TO SPEECH PROCESSING UNIT
90
92
94
ANNOUNCEMENT HARDWARE
ANNOUNCEMENT PROCESSING HARDWARE DRIVER
ANNOUNCEMENT PROCESSING UNIT
96
98
100
TO DATABASE MODULE 72

FIGURE 5

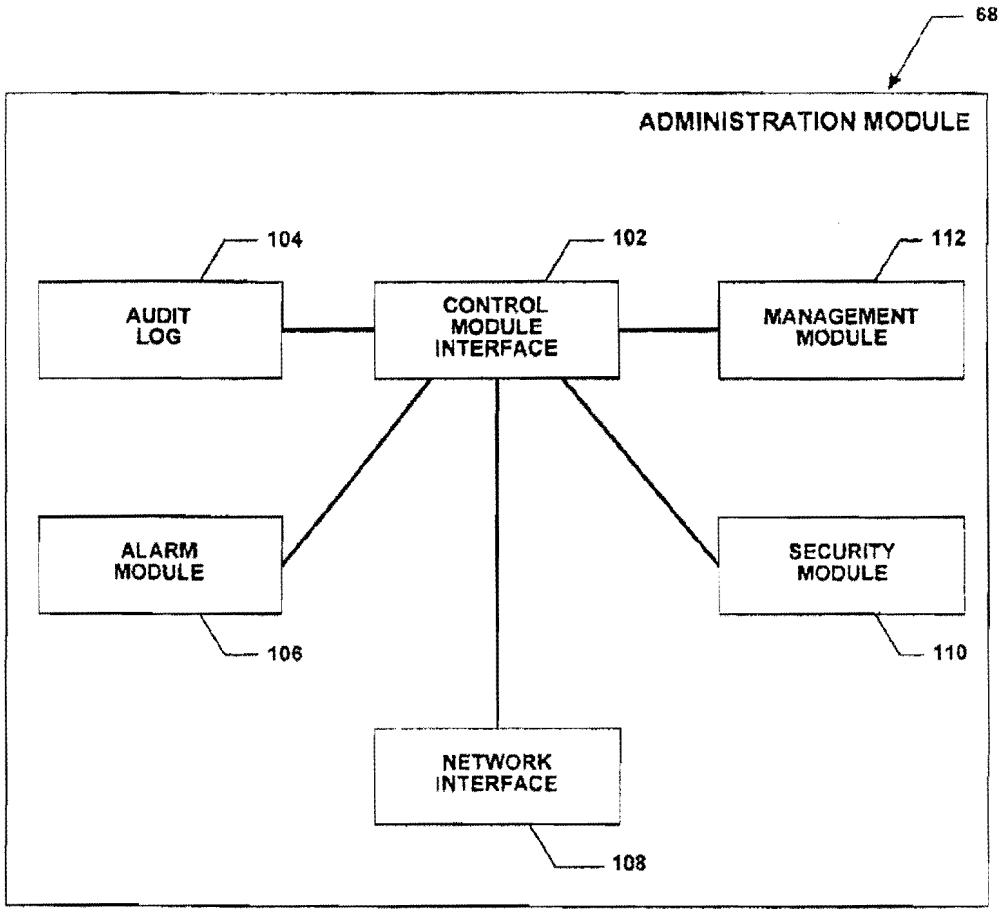

68
ADMINISTRATION MODULE
104
AUDIT LOG
102
CONTROL MODULE INTERFACE
112
MANAGEMENT MODULE
ALARM MODULE
106
SECURITY MODULE
110
NETWORK INTERFACE
108

FIGURE 6

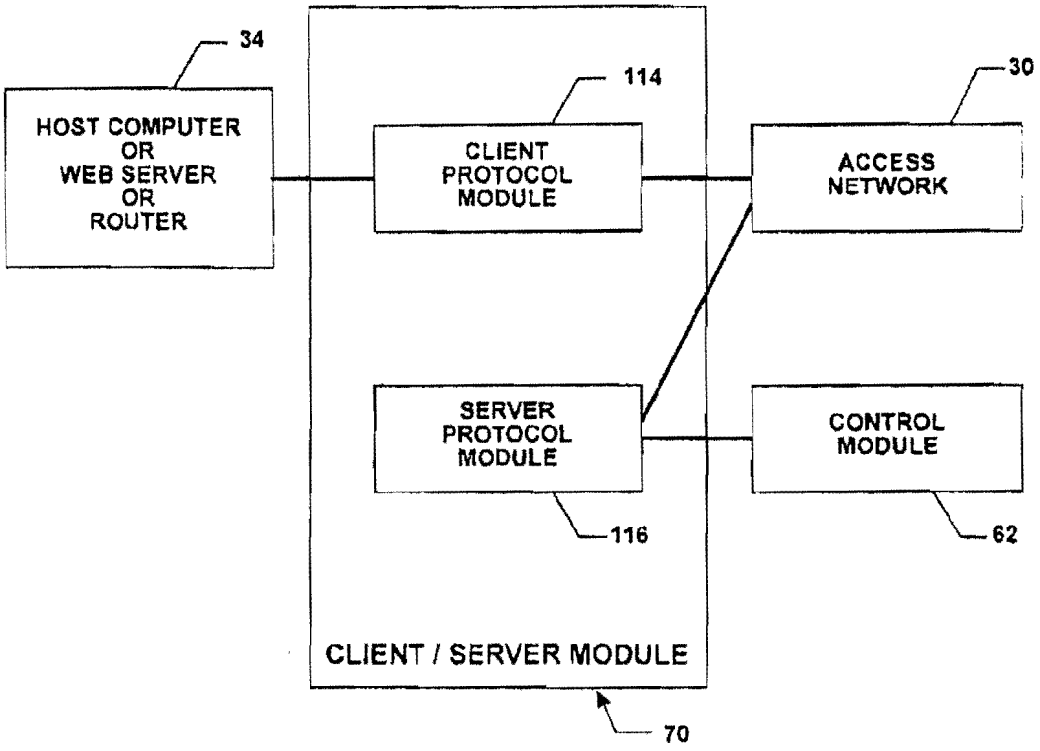

34
HOST COMPUTER
OR
WEB SERVER
OR
ROUTER
114
CLIENT
PROTOCOL
MODULE
30
ACCESS
NETWORK
SERVER
PROTOCOL
MODULE
116
CONTROL
MODULE
62
CLIENT / SERVER MODULE
70

FIGURE 7

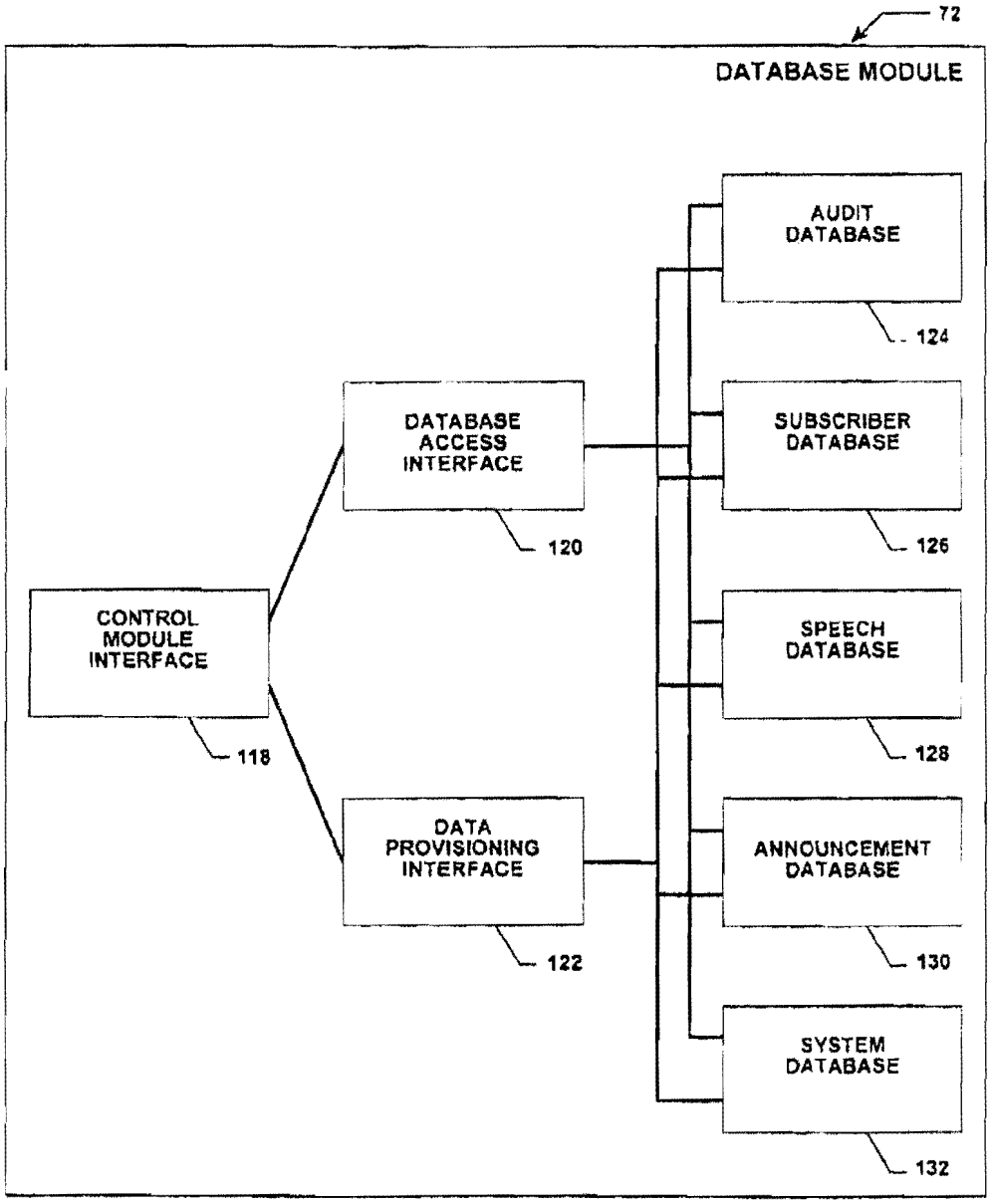

72
DATABASE MODULE
AUDIT DATABASE
124
DATABASE ACCESS INTERFACE
120
SUBSCRIBER DATABASE
126
CONTROL MODULE INTERFACE
118
SPEECH DATABASE
128
DATA PROVISIONING INTERFACE
122
ANNOUNCEMENT DATABASE
130
SYSTEM DATABASE
132

FIGURE 8

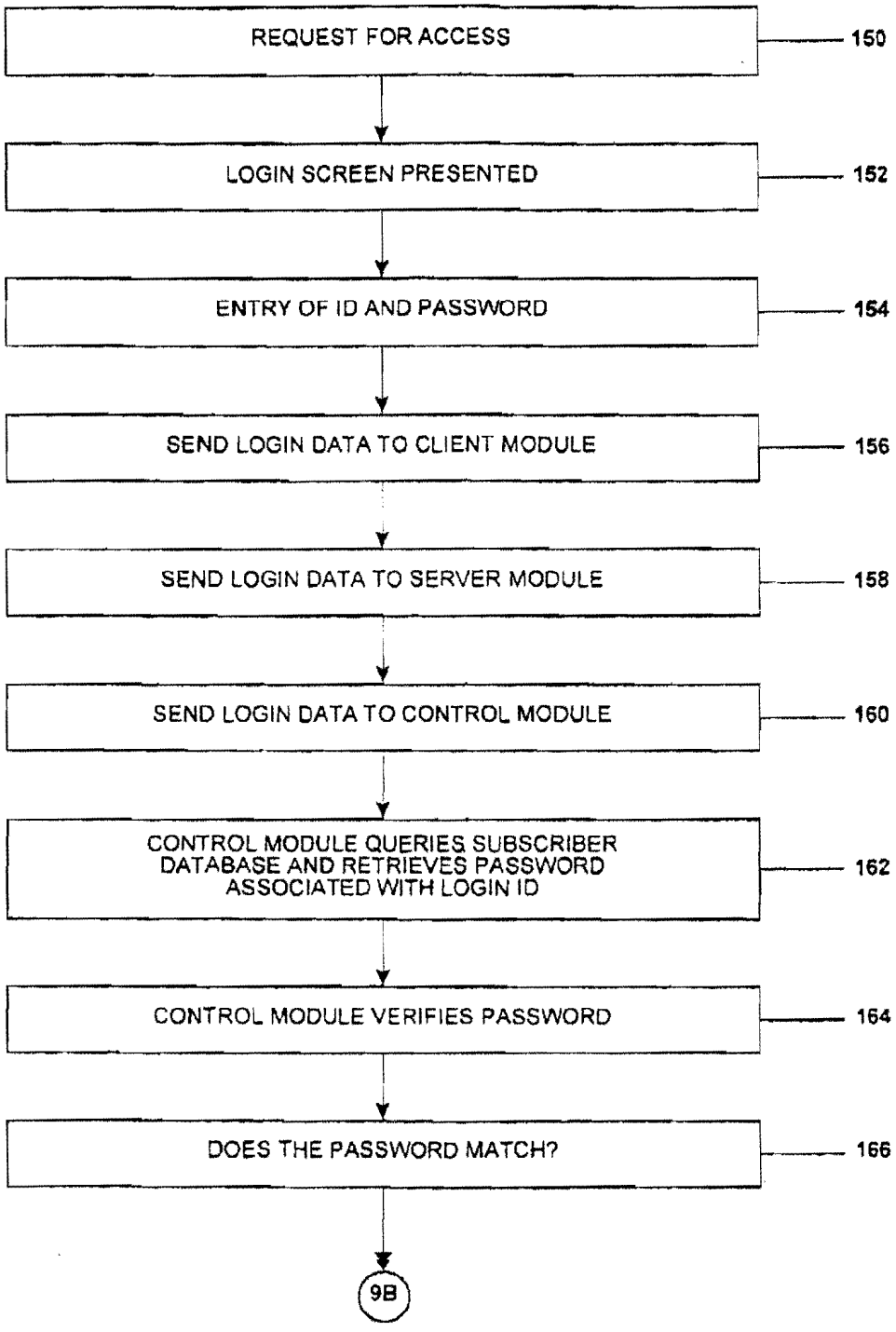

REQUEST FOR ACCESS
150
LOGIN SCREEN PRESENTED
152
ENTRY OF ID AND PASSWORD
154
SEND LOGIN DATA TO CLIENT MODULE
156
SEND LOGIN DATA TO SERVER MODULE
158
SEND LOGIN DATA TO CONTROL MODULE
160
CONTROL MODULE QUERIES SUBSCRIBER DATABASE AND RETRIEVES PASSWORD ASSOCIATED WITH LOGIN ID
162
CONTROL MODULE VERIFIES PASSWORD
164
DOES THE PASSWORD MATCH?
166
9B

FIGURE 9A

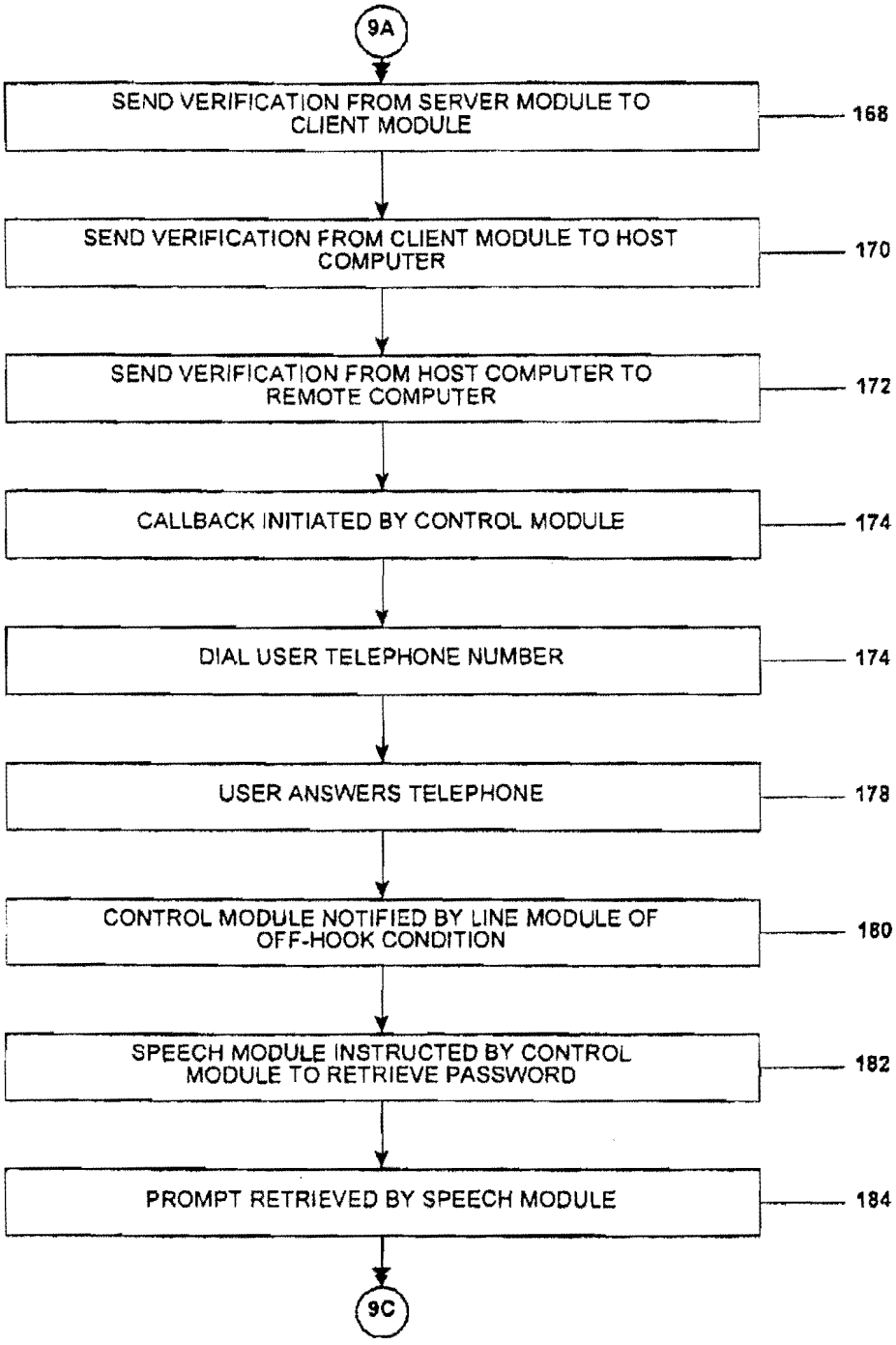

9A
SEND VERIFICATION FROM SERVER MODULE TO CLIENT MODULE
168
SEND VERIFICATION FROM CLIENT MODULE TO HOST COMPUTER
170
SEND VERIFICATION FROM HOST COMPUTER TO REMOTE COMPUTER
172
CALLBACK INITIATED BY CONTROL MODULE
174
DIAL USER TELEPHONE NUMBER
174
USER ANSWERS TELEPHONE
178
CONTROL MODULE NOTIFIED BY LINE MODULE OF OFF-HOOK CONDITION
180
SPEECH MODULE INSTRUCTED BY CONTROL MODULE TO RETRIEVE PASSWORD
182
PROMPT RETRIEVED BY SPEECH MODULE
184
9C

FIGURE 9B

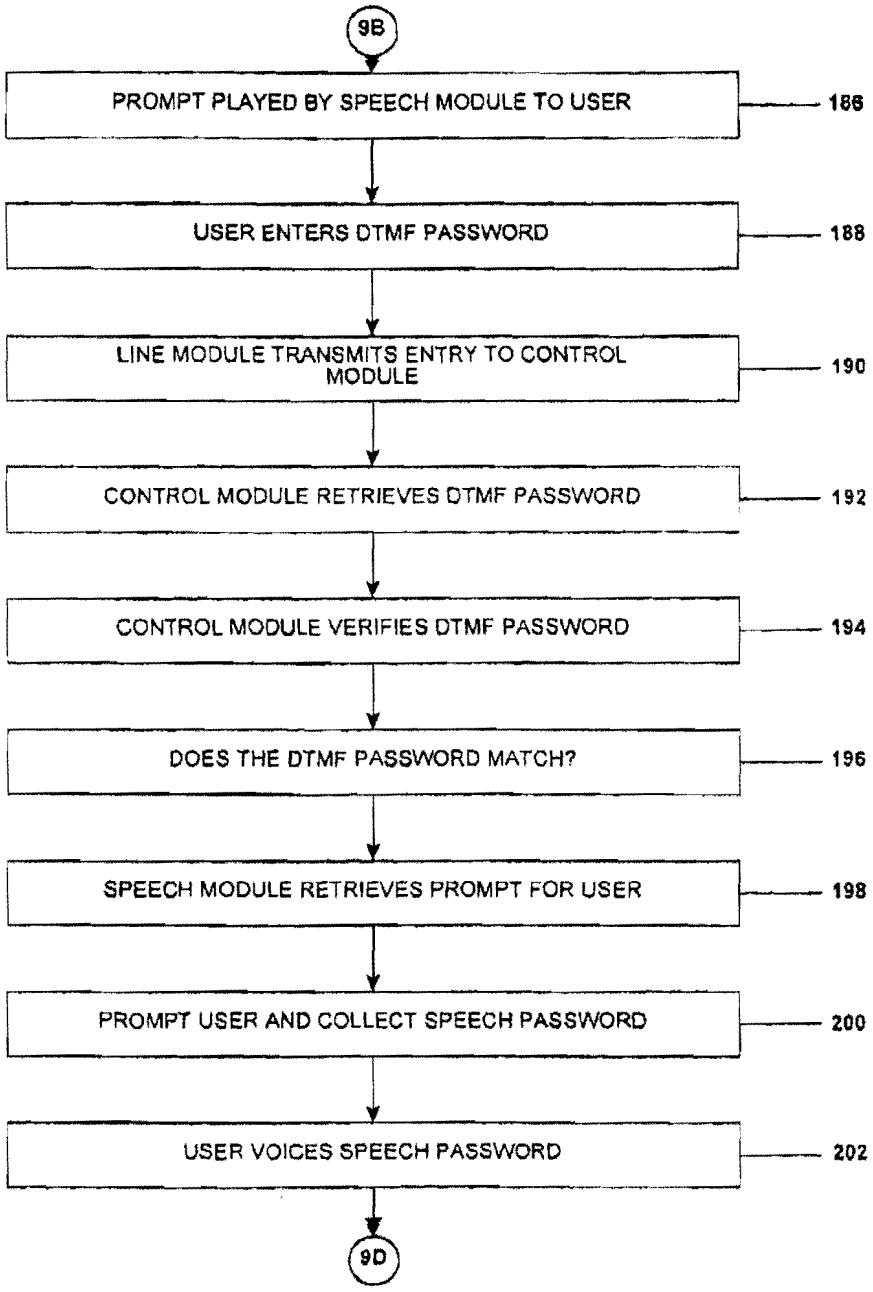

9B
PROMPT PLAYED BY SPEECH MODULE TO USER
186
USER ENTERS DTMF PASSWORD
188
LINE MODULE TRANSMITS ENTRY TO CONTROL MODULE
190
CONTROL MODULE RETRIEVES DTMF PASSWORD
192
CONTROL MODULE VERIFIES DTMF PASSWORD
194
DOES THE DTMF PASSWORD MATCH?
196
SPEECH MODULE RETRIEVES PROMPT FOR USER
198
PROMPT USER AND COLLECT SPEECH PASSWORD
200
USER VOICES SPEECH PASSWORD
202
9D

FIGURE 9C

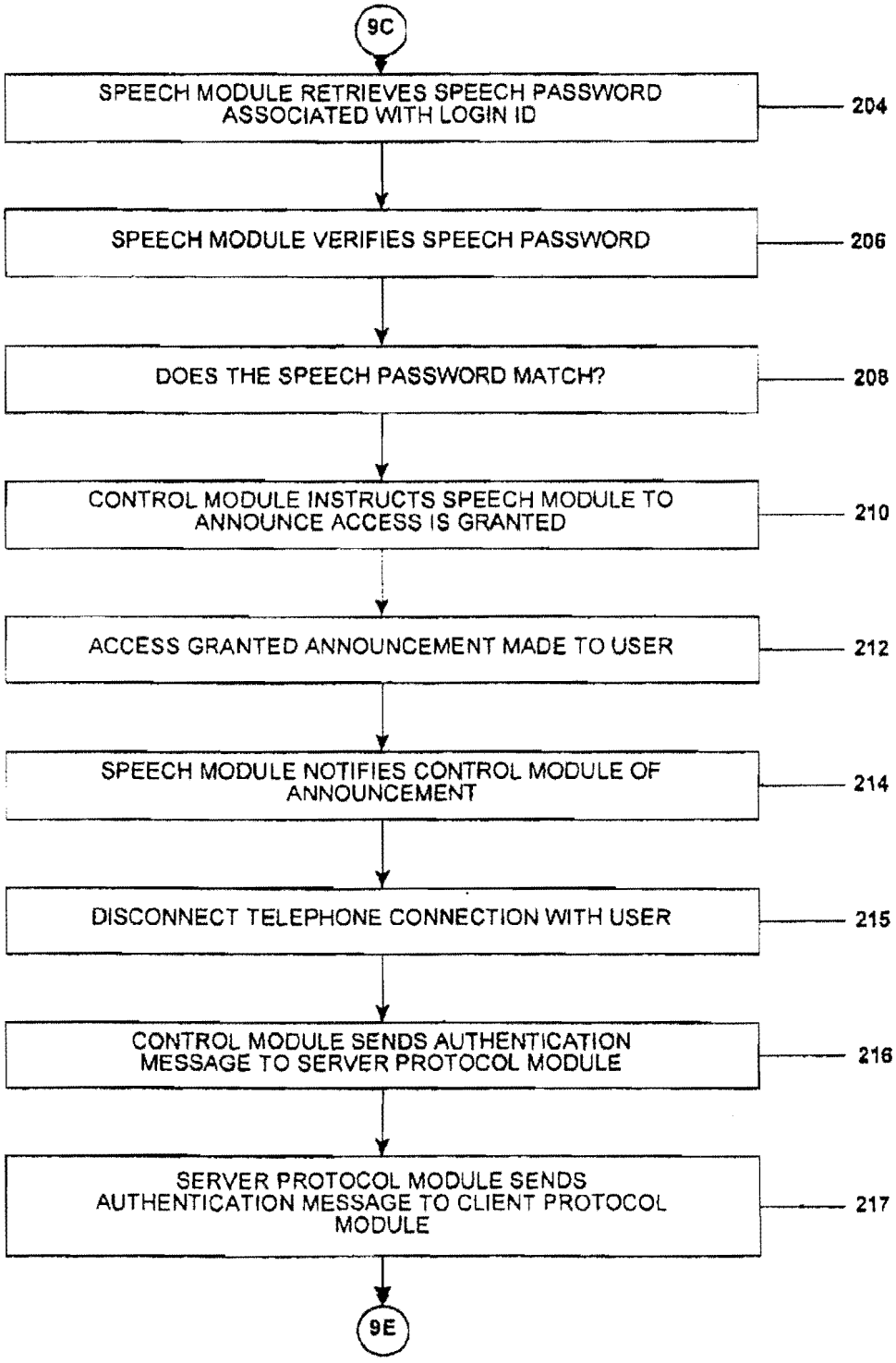

9C
SPEECH MODULE RETRIEVES SPEECH PASSWORD ASSOCIATED WITH LOGIN ID
204
SPEECH MODULE VERIFIES SPEECH PASSWORD
206
DOES THE SPEECH PASSWORD MATCH?
208
CONTROL MODULE INSTRUCTS SPEECH MODULE TO ANNOUNCE ACCESS IS GRANTED
210
ACCESS GRANTED ANNOUNCEMENT MADE TO USER
212
SPEECH MODULE NOTIFIES CONTROL MODULE OF ANNOUNCEMENT
214
DISCONNECT TELEPHONE CONNECTION WITH USER
215
CONTROL MODULE SENDS AUTHENTICATION MESSAGE TO SERVER PROTOCOL MODULE
216
SERVER PROTOCOL MODULE SENDS AUTHENTICATION MESSAGE TO CLIENT PROTOCOL MODULE
217
9E

FIGURE 9D

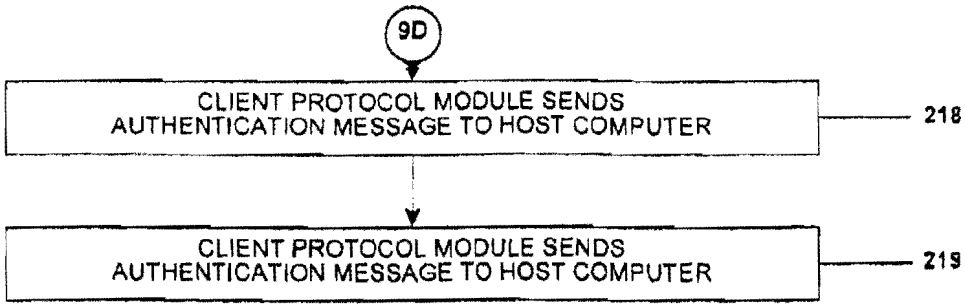

9D
CLIENT PROTOCOL MODULE SENDS AUTHENTICATION MESSAGE TO HOST COMPUTER
218
CLIENT PROTOCOL MODULE SENDS AUTHENTICATION MESSAGE TO HOST COMPUTER
219

FIGURE 9E

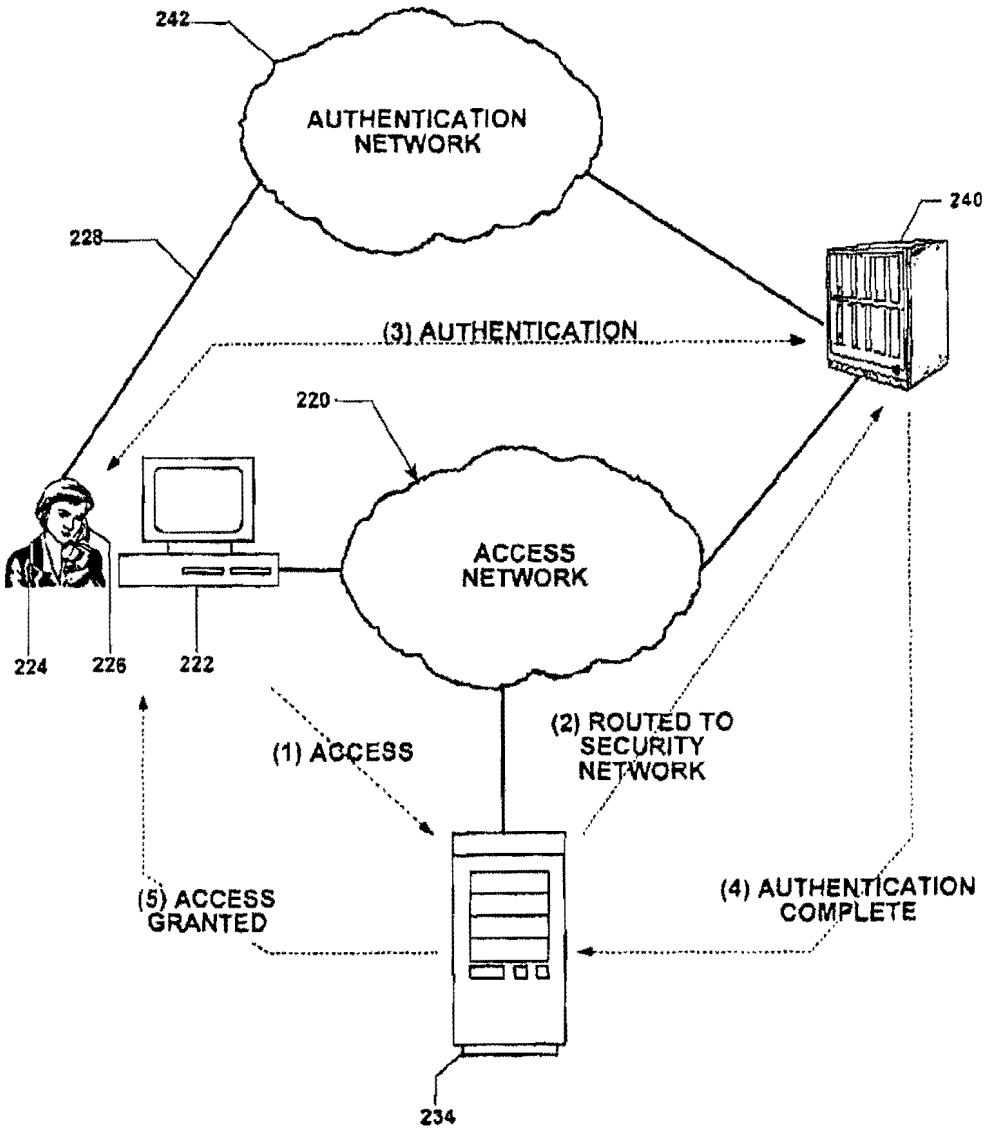

242
AUTHENTICATION NETWORK
240
228
(3) AUTHENTICATION
220
ACCESS NETWORK
224
226
222
(1) ACCESS
(2) ROUTED TO SECURITY NETWORK
(5) ACCESS GRANTED
(4) AUTHENTICATION COMPLETE
234

FIGURE 10

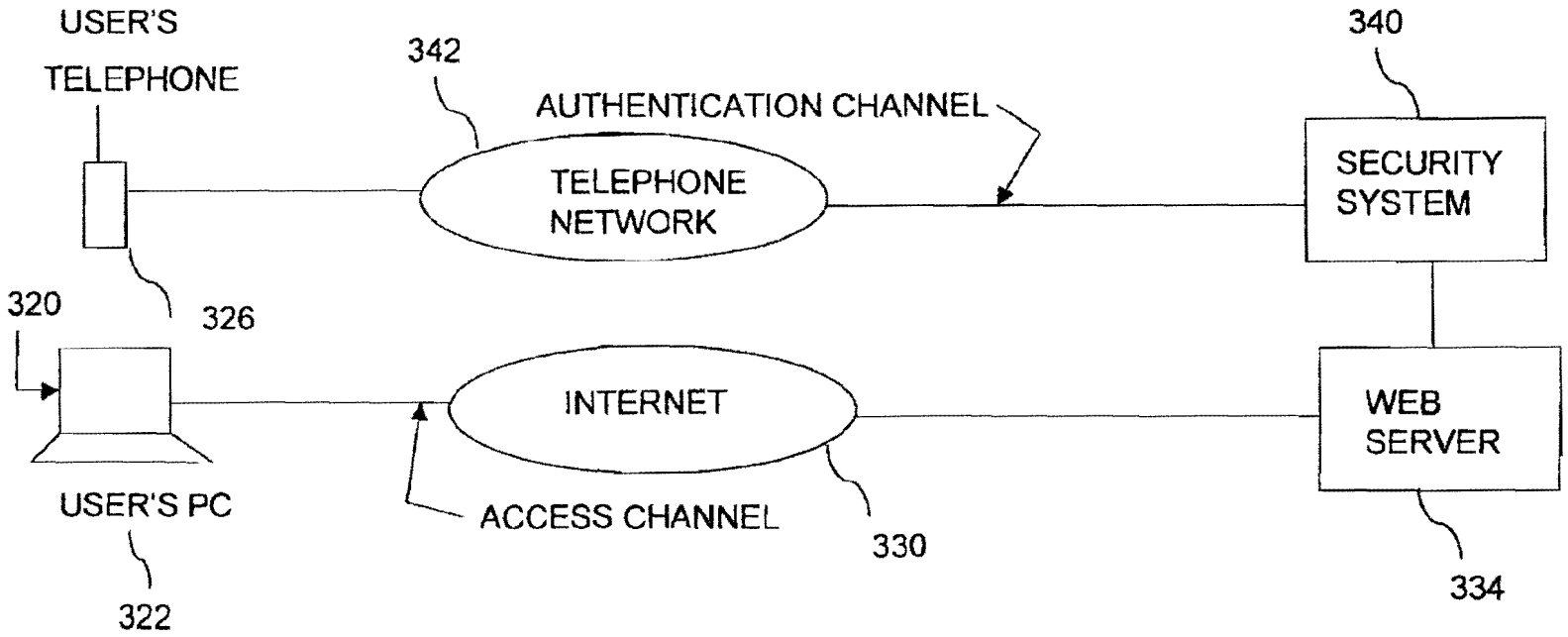

USER'S
TELEPHONE
342
AUTHENTICATION CHANNEL
340
TELEPHONE
NETWORK
SECURITY
SYSTEM
320
326
INTERNET
WEB
SERVER
USER'S PC
ACCESS CHANNEL
330
334
322

FIGURE 11

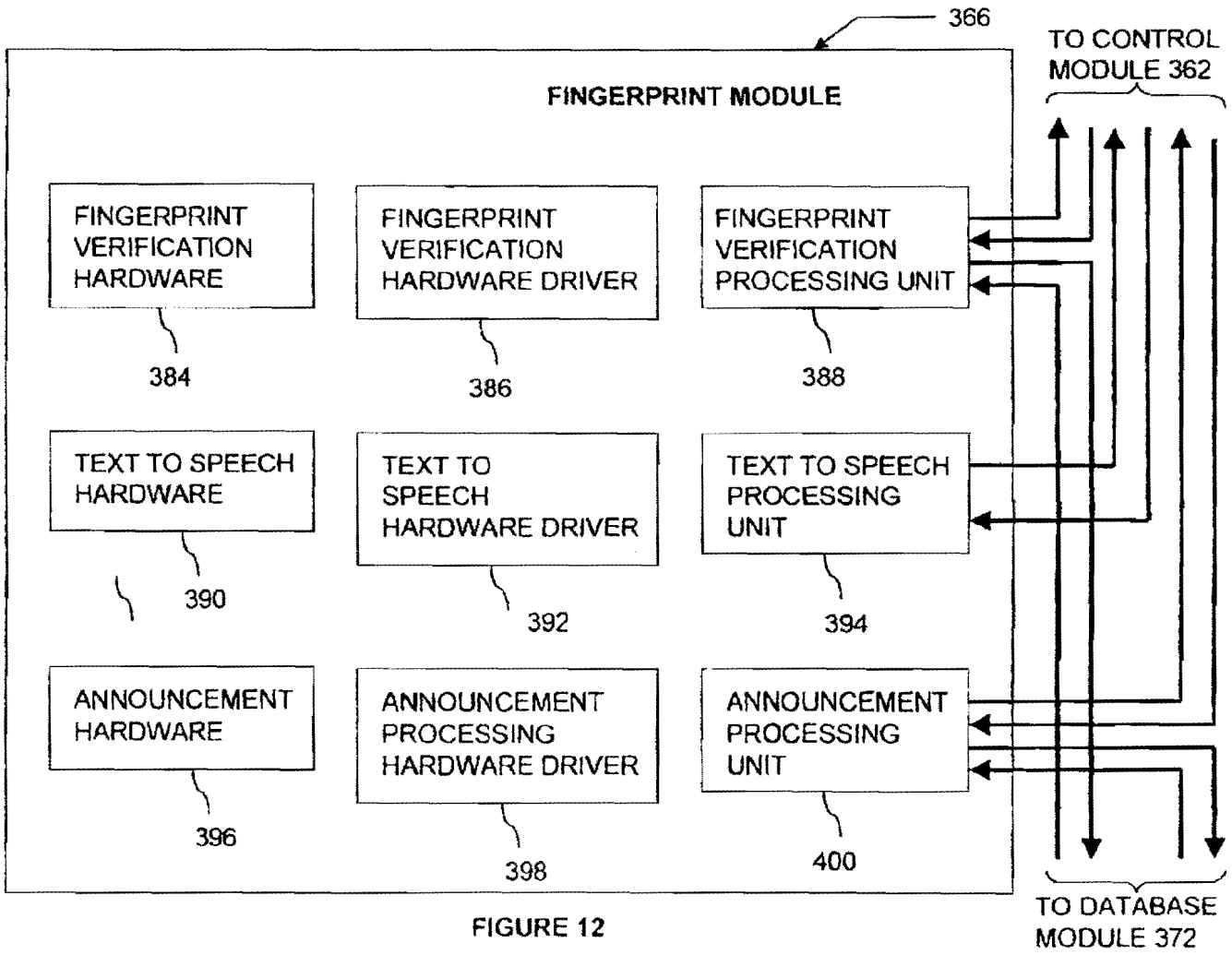

366
FINGERPRINT MODULE
FINGERPRINT VERIFICATION HARDWARE
384
FINGERPRINT VERIFICATION HARDWARE DRIVER
386
FINGERPRINT VERIFICATION PROCESSING UNIT
388
TEXT TO SPEECH HARDWARE
390
TEXT TO SPEECH HARDWARE DRIVER
392
TEXT TO SPEECH PROCESSING UNIT
394
ANNOUNCEMENT HARDWARE
396
ANNOUNCEMENT PROCESSING HARDWARE DRIVER
398
ANNOUNCEMENT PROCESSING UNIT
400
TO CONTROL MODULE 362
TO DATABASE MODULE 372

FIGURE 12

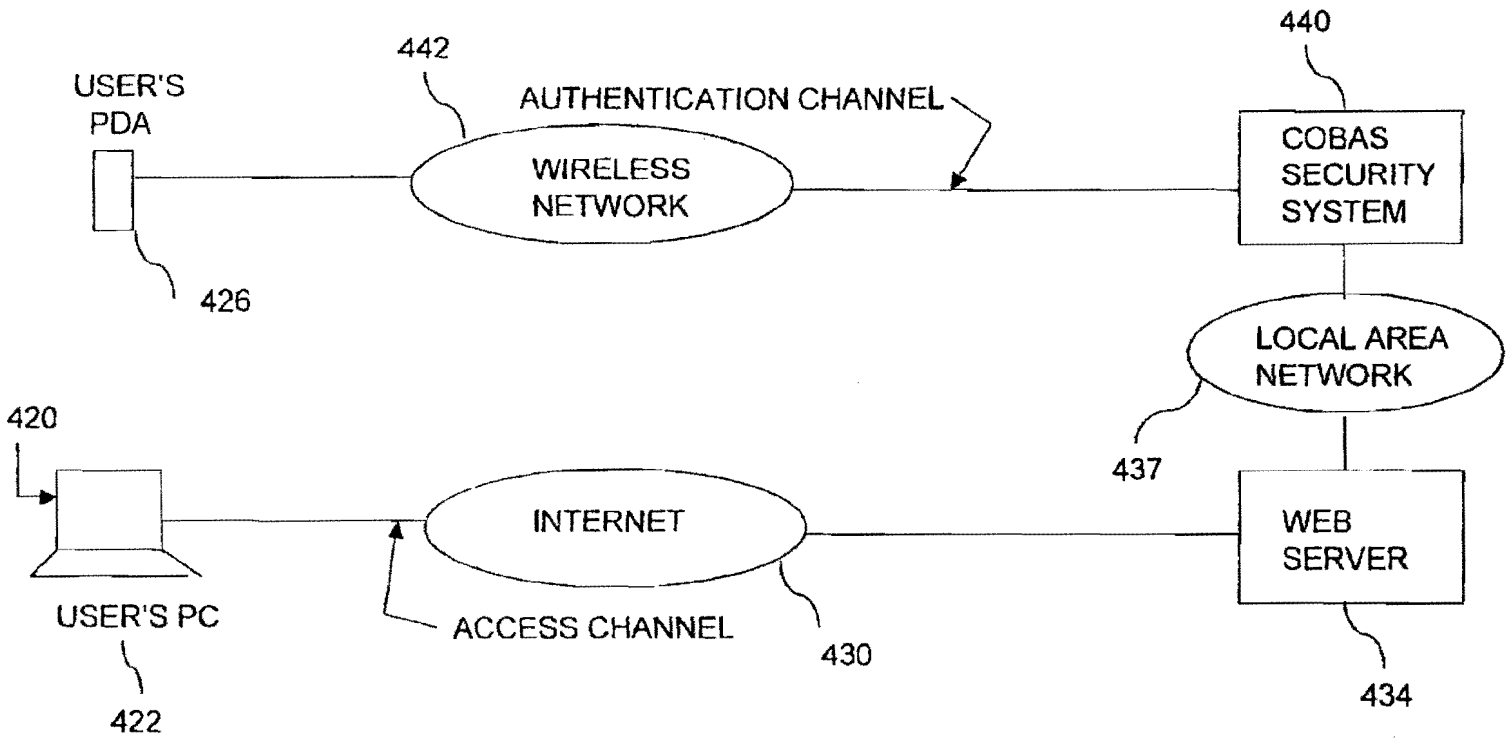

USER'S PDA
426
442
AUTHENTICATION CHANNEL
WIRELESS NETWORK
440
COBAS SECURITY SYSTEM
LOCAL AREA NETWORK
437
420
USER'S PC
422
INTERNET
ACCESS CHANNEL
430
WEB SERVER
434

FIGURE 13

MULTICHANNEL DEVICE UTILIZING A CENTRALIZED OUT-OF-BAND AUTHENTICATION SYSTEM (COBAS)

RELATED APPLICATION

This is a continuation-in-part of an application entitled OUT-OF-BAND SECURITY NETWORKS FOR COMPUTER NETWORK APPLICATIONS, Ser. No. 09/655,297, filed Sep. 5, 2000 and now abandoned. This application is incorporated herein by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates to security networks for computer network applications, and, more particularly, to a security network which provides user authentication by an out-of-band system that is entirely outside the host computer network being accessed. In addition, the out-of-band system optionally includes provision for biometric identification as part of the authentication process.

2. Background of the Invention

In the past, there have typically been three categories of computer security systems, namely, access control, encryption and message authentication, and intrusion detection. The access control systems act as the first line of defense against unwanted intrusions, and serve to prevent hackers who do not have the requisite information, e.g. the password, etc., from accessing the computer networks and systems. Secondly, the encryption and message authentication systems ensure that any information that is stored or in transit is not readable and cannot be modified. In the event that a hacker is able to break into the computer network, these systems prevent the information from being understood, and, as such, encryption systems as the second line of defense. Further intrusion detection systems uncover patterns of hacker attacks and viruses and, when discovered provide an alarm to the system administrator so that appropriate action can be taken. Since detection systems operate only after a hacker has successfully penetrated a system, such systems act as a third line of defense.

Obviously, as an access control system is the first line of defense, it is important that the selection thereof be well-suited to the application. In access control systems there is a broad dichotomy between user authentication and host authentication systems. In current practice, the most common user authentication systems include simple password systems, random password systems, and biometric systems. The simple password systems are ubiquitous in our society with every credit card transaction using a pin identification number, every automatic teller machine inquiry looking toward a password for access, and even telephone answering messages using simple password systems for control.

Additionally, when random password systems are used, another level of sophistication is added. In these systems, the password changes randomly every time a system is access. These systems are based on encryption or a password that changes randomly in a manner that is synchronized with an authorization server. The Secure ID card is an example of such a system. Random password systems require complimentary software and/or hardware at each computer authorized to use the network.

In biometric systems, characteristics of the human body, such as voice, fingerprints or retinal scan, are used to control access. These systems require software and/or hardware at each computer to provide authorization for the use of the network.

Another category of access control is that of host authentication. Here the commonest systems are those of "callback" and "firewall" systems. Callback systems are those systems which work by calling a computer back at a predetermined telephone number. These systems authenticate the location of a computer and are suitable for dial-up (modem) networks; however, such systems are ineffective when the attack comes via the Internet. On the other hand, firewall systems are designed to prevent attacks coming from the Internet and work by allowing access only from computers within a network. Even though firewall systems are implemented either as standalone systems or incorporated into routers, skilled hackers are able to penetrate host authentication systems.

Typically, access-control security products, as described above, are in-band authentication systems with the data and the authentication information on the same network. Thus, upon accessing a computer, a computer prompt requests that you enter your password and, upon clearance, access is granted. In this example, all information exchanged is on the same network or in-band. The technical problem created thereby is that the hacker is in a self-authenticating environment.

Except for callback systems, the above access control products authenticate only the user and not the location. When computer networks could only be accessed by modems, the authentication of location by dialing back the access-requesting computer, provided a modicum of security. Now, as virtually all computer networks are accessible by modem-independent internet connection, location authentication by callback is no longer secure. The lack of security arises as there is no necessary connection between the internet address and a location, and, in fact, an internet address most often changes from connection to connection. Thus, callback systems are rendered useless against attacks originating from the internet.

In preparing for this application, a review of various patent resources was conducted. The review resulted in the inventor gaining familiarity with the following patents:

Item No.	Pat. No.	Inventor	Orig. Class	Date
1	6,408,062	Cave, Ellis K.	379/210.01	June 2002
2	5,901,284	Handy-Swink, Katheryn A.	713/200	May 1999
3	5,898,830	Wesinger, Jr. et al.	395/187.01	April 1999
4	5,872,834	Teitelbaum	379/93.03	February 1999
5	5,826,014	Coley, et al.	718.301	October 1998
6	5,787,187	Bouchard	382/115	July 1998
7	5,680,458	Spelman, et al.	380/21	October 1997
8	5,621,809	Bellegarda, et al.	382/116	April 1997
9	5,615,277	Hoffman	382/115	March 1997
10	5,588,060	Aziz	380/30	December 1996
11	5,548,646	Aziz, et al.	380/23	August 1996
12	5,153,918	Tuai, Gregory	713/182	October 1992

In general terms, the patents all show a portion of the authentication protocol and the data transferred in the same channel or "in-band". For purposes of this discussion "in-band" operation is defined as one conducted wholly within a single channel or loop. Likewise, an "out-of-band" operation is defined as one using an authentication channel that is separated from the channel carrying the information and therefore is nonintrusive as it is carried over separate facilities, frequency channels, or time slots than those used for actual information transfer.

The patent to E. K. Cave, U.S. Pat. No. 6,408,062, Item 1 above, describes a callback system. Here, the user is prequali-

fied so that he does not get charged for calls that are not completed to the called party. However, here the authentication and the administrative function are in the same loop.

In Item 3, the patent to Wesinger et al., U.S. Pat. No. 5,898,830 ('830) is a firewall patent. Here, the inventor attempts to enhance security by using out-of-band authentication. In his approach, a communication channel, or medium, other than the one over which the network communication takes place, is used to transmit or convey an access key. The key is transmitted from a remote location (e.g., using a pager or other transmission device) and, using a hardware token, the key is conveyed to the local device. In the Wesinger '830 system, to gain access, a hacker must have access to a device (e.g., a pager, a token, etc.) Used to receive the out-of-band information. Pager beep-back or similar authentication techniques may be especially advantageous in that, if a hacker attempts unauthorized access to a machine while the authorized user is in possession of the device, the user will be alerted by the device unexpectedly receiving the access key. The key is unique to each transmission, such that even if a hacker is able to obtain it, it cannot be used at other times or places or with respect to any other connection.

Next, turning to Item 7, the patent to Spelman et al., U.S. Pat. No. 5,680,458 ('458), a method of recovering from the compromise of a root key is shown. Here, following the disruption of a new replacement key, an out-of-band channel is used by a central authority to publish a verification code which can be used by customers to verify the authenticity of the emergency message. The Spelman '458 patent further indicates that the central authority uses the root key to generate a digital signature which is appended to the emergency message to verify that the emergency message is legitimate.

Hoffman, U.S. Pat. No. 5,615,277, Item 9, is next discussed. Here, biometrics are combined with a tokenless security and the patent describes a method for preventing unauthorized access to one or more secured computer systems. The security system and method are principally based on a comparison of a unique biometric sample, such as a voice recording, which is gathered directly from the person of an unknown user with an authenticated unique biometric sample of the same type. The Hoffman technology is networked to act as a full or partial intermediary between a secured computer system and its authorized users. The security system and method further contemplate the use of personal codes to confirm identifications determined from biometric comparisons, and the use of one or more variants in the personal identification code for alerting authorities in the event of coerced access.

Items 10 and 11 have a common assignee, Sun Microsystems, Inc., and both concern encryption/decryption keys and key management.

The patent to Tuai, U.S. Pat. No. 5,153,918 ('918) describes an in-band authentication system which uses a callback system after authentication. Within the authentication system, Tuai '918 employs a voice verification technique.

The submission of the above list of documents is not intended as an admission that any such document constitutes prior art against the claims of the present application. Applicant does not waive any right to take any action that would be appropriate to antedate or otherwise remove any listed document as a competent reference against the claims of the present application. None of the above show the novel and unobvious features of the invention described hereinbelow.

SUMMARY

In general terms, the invention disclosed hereby includes in the embodiments thereof, a unique combination of user and host authentication. The security system of the present invention is out-of-band with respect to the host computer and is configured to intercept requests for access. The first step in controlling the incoming access flow is a user authentication provided in response to prompts for a user identification and password. After verification at the security system, the system operating in an out-of-band mode, uses telephone dialup for location authentication and user authentication via a password entered using a telephone keypad. In addition and optionally the system provides further authentication using a biometric system. When voice recognition is employed for the biometric component, the user speaks a given phrase which the system authenticates before permitting access. Upon granting of access, the user now for the first time enters the in-band operating field of the host computer.

OBJECT AND FEATURES OF THE INVENTION

It is an object of the present invention to provide a host computer with a cost effective, out-of-band security network that combines high security and tokenless operation.

It is a further object of the present invention to provide a network to isolate the authentication protocol of a computer system from the access channel therefor.

It is yet another object of the present invention to provide a separate security network which acts conjunctively with or as an overlying sentry box to the existing security system provided by the host computer.

It is still yet another object of the present invention to provide an authentication using a biometric component, such as speech recognition, to limit access to specific individuals.

It is a feature of the present invention that the security network achieves high security without encryption and decryption.

It is another feature of the present invention to have a callback step that restricts authentication to a given instrument thereby enabling restriction to a fixed location.

It is yet another feature of the present invention to combine callback and speech recognition in an out-of-band security facility.

Other objects and features of the invention will become apparent upon review of the drawings and the detailed description which follow.

BRIEF DESCRIPTION OF THE DRAWINGS

In the following drawings, the same parts in the various views are afforded the same reference designators.

FIG. 1 is a schematic diagram of the prior art security system;

FIG. 1A is a schematic diagram of the security system of the present invention as applied to the internet in which an external accessor in a wide area network seeks entry into a host system;

FIG. 2 is a schematic diagram of the apparatus required for the security system shown in FIG. 1;

FIG. 3 is a schematic diagram of the software program required for the security system shown in FIG. 1 in which

various program modules are shown for corresponding functions of the system and each module is shown in relation to the control module thereof;

FIG. **4** is a detailed schematic diagram of the software program required for the line module of the security system shown in FIG. **3**;

FIG. **5** is a detailed schematic diagram of the software program required for the speech module of the security system shown in FIG. **3**;

FIG. **6** is a detailed schematic diagram of the software program required for the administration module of the security system shown in FIG. **3**;

FIG. **7** is a detailed schematic diagram of the software program required for the client/server module of the security system shown in FIG. **3**;

FIG. **8** is a detailed schematic diagram of the software program required for the database module of the security system shown in FIG. **3**;

FIG. **9**A through **9**E is a flow diagram of the software program required for the security system shown in FIG. **1**;

FIG. **10** is a schematic diagram of a second embodiment of the security system of the present invention as applied to the intranet in which an internal accessor in a local area network seeks entry into a restricted portion of the host system;

FIG. **11** is a schematic diagram of the third embodiment of the security system using as peripheral devices a cellular telephone and a fingerprint verification device;

FIG. **12** is a detailed schematic diagram of the software program required for the fingerprint module of the security system shown in FIG. **11**; and,

FIG. **13** is a detailed schematic diagram of the fourth embodiment of the security system using as peripheral devices a personal digital assistant (PDA) and the associated fingerprint verification device.

DESCRIPTION OF THE PREFERRED EMBODIMENT

In the description that follows, the prior art is shown in FIG. **1**. In a typical call-back system which this epitomizes, the user from his computer **10** accesses through an optional voice encoder **12** and, along a single authentication channel. The channel includes an in-band arrangement of the user's modem **14**, the host computer modem **16** and the authentication controller **17**. In a specific example of this, in the Tuai '918 system, see supra, which uses voice verification, the user accesses a host computer **18** via modems **14** and **16**. The access attempt is intercepted by the controller **17** which prompts the user to enter a USER ID and speak a phrase for voice verification. If the verification is successful, the controller **17** acting within the single communication channel connects the user computer to the host computer. Both the USER ID and the voice password are sent along the same pathway and any improper accessor into this channel has the opportunity to monitor and/or enter both identifiers.

The out-of-band security system networks for computer network applications is described in two embodiments. The first describes an application to a wide area network, such as the internet, wherein the person desiring access and the equipment used thereby are remote from the host computer. In this description and consistent with Newton's *Telecom Dictionary* (19th Ed.), an "out-of-band" system is defined herein as one having an authentication channel that is separated from the information channel and therefore is nonintrusive as it is carried over separate facilities than those used for actual information transfer. The second embodiment describes the application of the disclosed invention to a local area network wherein the person desiring access and the equipment used thereby are within the same network (referred to as the "corporate network") as the host computer. For purposes of this description the person desiring access and the equipment used thereby are referred collectively as the "accessor".

In FIG. **1**, a general overview of the first embodiment of the out-of-band security networks for computer network applications of this invention is shown and is referred to generally by the reference designator **20**. Here the accessor is the computer equipment **22**, including the central processing unit and the operating system thereof, and the person or user **24** whose voice is transmittable by the telephone **26** over telephone lines **28**. The access network **30** is constructed in such a manner that, when user **24** requests access to a web page **32** located at a host computer or web server **34** through computer **22**, the request-for-access is diverted by a router **36** internal to the corporate network **38** to an out-of-band security network **40**. Authentication occurs in the out-of-band security network **40**, which is described in detail below.

This is in contradistinction to present authentication processes as the out-of-band security network **40** is isolated from the corporate network **38** and does not depend thereon for validating data. The first shows a biometric validation which, in this case, is in the form of voice recognition and is within voice network **42**. While voice recognition is used herein, it is merely exemplary of many forms of recognizing or identifying an individual person. Others include, but are not limited to fingerprint identification, iris recognition, retina identification, palms recognition, and face recognition. Each of these are similar to the first embodiment in that these are a requirement for monitoring the particular parameter of the individual person; including the parameter to a mathematical representation or algorithm therefore; retrieving a previously stored sample (biometric data), thereof from a database and comparing the stored sample with the input of the accessor.

Referring now to FIG. **2** a block diagram is shown for the hardware required by the out-of-band security network for computer network applications of this invention. The request-for-access is forwarded from the router **36** of the corporate network to a data network interface **50** which, in turn, is constructed to transfer the request to a dedicated, security network computer **52** over a data bus **48**. The computer **52** is adapted to include software programs, see infra, for receiving the user identification and for validating the corresponding password, and is further adapted to obtain the user telephone number from lookup tables within database **54** through data bus **48**. The computer **52** is equipped to telephone the user through a PBX interface **56** and voice bus **58**. For voice recognition, a speech or biometric system **60** is provided to process requested speech phrases repeated by the user **24** which is verified within the security computer **52**. Upon authentication, access is granted through the data network interface **50**.

Referring now to FIGS. **3** through **8** the software architecture supporting the above functions is next described. The security computer **52**, FIG. **2**, is structured to include various functional software modules, FIG. **3**, namely, a control module **62**, a line module **64**, a speech module including a biometric for voice recognition **66**, an administration module **68**, a client/server module **70**, and a database module **72**. The software program of the control module **62** functions and interconnects with the other modules (line, speech, administration, client/server and database modules) to control the processing flow and the interfacing with the internal and external system components.

As will be understood from the flow diagram description, infra, the control module **62** software of the security computer

52 incorporates a finite state machine, a call state model, process monitors, and fail-over mechanisms. The software program of the line module 64 is structured to provide an interface with the telephone network. The software program of the speech module 66 is structured to perform processing functions such as, but not limited to, speech verification, text-to-speech conversion and announcements. The software program of the administration module 68 is structured to archive the records of each call made, to provide security and management functions, and to process any alarms generated. The software program of the client/server module 70 is structured to enable a host computer or a web server 34 to interface with the out-of-band security network 40. The software program of the database module 72 is comprised of the databases to support the security network 40 which in the present invention includes an audit database, a subscriber database, a speech database, an announcement database, and a system database.

Referring now to FIG. 4, the line module 64 is described in further detail. The analog telephone interface 74 is the equipment, such as voice bus 58 and PBX interface 56, that interfaces to an analog line. The analog telephone interface 74 is, in turn, controlled by software program of the analog line driver 76. Similarly, digital telephone interface 78 is the equipment, such as data bus 48 and PBX interface 56, that interfaces to a digital line (T1 or ISDN PRI)a. The digital telephone interface 78 is, in turn, controlled by the software program of the digital line driver 80. The software program of the telephone functions module 82 is structured to accommodate functions such as, Call Origination, Call Answer, Supervisory signaling, Call Progress signaling, Ring generation/detection, DTMF generation/detection, and line configuration.

In FIG. 5 the speech module 66 architecture is detailed. The speech verification (SV) hardware 84, (part of speech system 60, FIG. 2) consists of digital signal processors that utilize SV algorithms for verification of an accessor's spoken password. The speech verification hardware 84 is controlled by the software program of the SV hardware driver 86. The software program of the speech verification processing unit 88 provides an interface with control module 62 and is structured to respond to queries therefrom for verifying an accessor's spoken password. Also, the SV processing unit 88 enables the enrollment of users with the speech password and the interaction of the speech database of database module 72.

The text-to-speech (TTS) hardware 90 consists of digital signal processors that utilize TTS algorithms. The text-to-speech hardware 90 is controlled by the software program of the TTS hardware driver 92. The software program of the TTS processing unit 94 provides an interface with the control module 62 and, as required by the control module 62, converts text strings to synthesized speech. The announcement hardware 96 consists of digital signal processors that utilize speech algorithms to record and play announcements. The announcement hardware is controlled by the software program of the announcement hardware driver 98. The software program of the announcement processing unit 100 also provides an interface with control module 62; upon demands of the control module 62, supplies stored announcements; and interacts with the announcements database of database module 72.

In FIG. 6, the software program of the administration module 68 is presented in more detail. As the administration module 68 interfaces with the control module 62, see supra, a subprogram, namely, a control module interface 102 is constructed to manage the communication therebetween. The administration module 68 further includes software to provide an audit trail of all calls requesting access. This unit or audit log 104 creates records about each call, which records are stored in the audit database of the database module 72. Any alarms caused as a result of errors, threshold crossing or system failures are processed by the software program of alarm module 106. For remote administration of the out-of-band security system 40 of this invention, the software program of the network interface 108 is provided, which software communicates with the corporate network 38 (via network adapters). Access to the out-of-band security system 40 for administrative purposes is controlled by security module 110. Similar to the network interface 108, the software program of the management module 112 provides for the remote management of the out-of-band security system 40 for configuration, status reporting, software upgrades and trouble-shooting purposes.

Referring now to FIG. 7, the software program of the client/server module 70 that secures the host computer or web server or router 34 of the corporate network 38 through the out-of-band security system 40 of this invention is shown in detail. Here, the client protocol module 114 provides the interfacing means for the host computer or web server 34 and communicates with the out-of-band security system 40 using a proprietary protocol. Alternatively, standard protocols such as RADIUS and TACACS can be used. The server protocol module 116 interfaces with the control module 62 and manages the interaction with the client protocol module 114.

In FIG. 8 a detailed schematic diagram is shown of the software program required for the database module 72 of the out-of-band security system 40 of this invention. The database module 72 is the recordkeeping center, the lookup table repository, and the archival storehouse of the system. In the above description numerous relationships to this module have already been drawn. The database module 72 communicates through control module interface 118 to the control module 62.

Two types of communications are channeled to and from the database module 72, namely, communicating data for use during operations through database access interface 120 and communicating data for maintenance and provisioning of the out-of-band security system through database provisioning interface 122. While the databases described herein are specifically related to the application of this embodiment to voice recognition the formation of specific databases, e.g. a different set of samples of biometric parameters or characteristics, is within the contemplation of the invention. The databases hereof are the audit database 124 for the call records; the subscriber database 126 for subscriber information; the speech database 128 for aid in verifying an accessor's spoken password; the announcements database 130 for announcements to be played to users during a call; and, system database 132 for system related information (e.g. configuration parameters).

In FIGS. 9A through 9E the flow diagram for the above software program operation is shown and is described hereinbelow. Thus, while the preceding in discussing the network architecture for the out-of-band security system 40 explains the access portion of the program—the operations side—and the configuration and maintenance portion of the program—the provisioning side, the description which follows is of the software operation of the out-of-band security system 40 from the receipt of a request-to-access inquiry to a granting-of-access or denial-of-access result. The logic description that follows reflects the accessor's inputs and the programmed processes along the logical pathway from the receipt of a request-to-access inquiry to a granting-of-access or denial-of-access result.

The pathway commences at the REQUEST FOR ACCESS block **150** whereby a request to enter the host computer or web server **34** is received from the user at the remote computer **22**. The user requesting access to the host computer from the remote computer is immediately prompted to login at the LOGIN SCREEN PRESENTED block **152**. While the login procedure here comprises the entry of the user identification and password and is requested by the host computer **34**, such information request is optionally a function of the security computer **40**. Upon entry of data by user at the ENTRY OF ID AND PASSWORD block **154** the information is passes to the security computer **40**.

As described in the software architecture review, supra, the software pathway of the login data is first to client module **114** at SEND LOGIN DATA TO CLIENT MODULE block **156** and then successively to server module **116** at SEND LOGIN DATA TO SERVER MODULE block **158** and to control module **62** at SEND LOGIN DATA TO CONTROL MODULE block **160**. In transmitting the login data from the client module **114** to the server module a proprietary protocol is employed, which protocol includes encryption of the data using standard techniques. The verification process is continued at the control module **62** which next enters the subscriber database **126** and retrieves at CONTROL MODULE QUERIES SUBSCRIBER DATABASE AND RETRIEVES PASSWORD ASSOCIATED WITH LOGIN ID block **162** the password associated with the logged in identification. The control module **62** verifies at CONTROL MODULE VERIFIES PASSWORD block **164** that the password received from the remote computer **22** is the same as the password retrieved from the subscriber database **126**.

Upon verification, the control module **62** at DOES THE PASSWORD MATCH? block **166** sends confirmation thereof back along the software pathway to inform the user of the event. Upon failure to verify, the control module **62** at DOES THE PASSWORD MATCH? block **166** initiates an alarm indicating that the login conditions were not met. The software program upon an alarm condition terminates processing. Alternatively, the program offers the user an opportunity to retry whereupon there is a retracement through the same software path as just described and then, upon repeated alarm occurrence, the software terminates processing. The retry process may be limited to a specified number of times. The message that the verification has been achieved is transmitted along the software pathway substantially in the reverse manner as the login data transmission.

From the control module **62**, the verification is first received by the server module **116** and at SEND VERIFICATION FROM SERVER MODULE TO CLIENT MODULE block **168** the verification message along with the information that the authentication is proceeding is transmitted to the client module **114**. In transmitting these messages to the client module **114** from the server module a proprietary protocol is employed, which protocol includes decryption of the data, where required, using standard techniques. The client module **114** transmits at SEND VERIFICATION FROM CLIENT MODULE TO HOST COMPUTER block **170** the message to the host computer **34**. Finally, the host computer **34** transmits at SEND VERIFICATION FROM HOST COMPUTER TO REMOTE COMPUTER block **172** the message that the login verification is complete is sent to the remote computer **22** and prompts the person or user **24** to stand by for a telephonic callback.

Now with the control module **62** having verified the remote computer **22**, the software program hereof is constructed to have the control module **62** at CALLBACK INITIATED BY CONTROL MODULE block **174** initiate out-of-band the call-back procedure to the user **24**. The control module **62** queries the subscriber database **126** and retrieves therefrom the telephone number associated with the login identification. Based on the data retrieved from the subscriber database, the control module **62** instructs the line module **64** at DIAL USER TELEPHONE NUMBER block **176** to call user **24**. Upon user **24** answering the telephone at USER ANSWERS TELEPHONE block **178**, the software pathway continues with the line module **64** relaying to the control module **62** at CONTROL MODULE NOTIFIED BY LINE MODULE OF OFF-HOOK CONDITION block **180** that the user's telephone is off-hook. The program is constructed so that the control module **62** then instructs the speech module **66** at SPEECH MODULE INSTRUCTED BY CONTROL MODULE TO RETRIEVE PASSWORD block **182** to retrieve (or generate) a DTMF password. To accomplish this, the speech module **66** now queries the announcement database **130** at PROMPT RETRIEVED BY SPEECH MODULE block **184** retrieves the prompt to be played to the user **24**. Alternatively, the password for the prompt is generated and synthesized by the text-to-speech system **90**, **92** and **94** of the speech module **66**.

At PROMPT PLAYED BY SPEECH MODULE TO USER block **186**, the user **24** is instructed to impress the DTMF password on the telephone keypad. The program progresses so that after the user **24** enters the DTMF password on the telephone keypad at USER ENTER DTMF PASSWORD block **188**, the line module **64** at LINE MODULE TRANSMITS ENTRY TO CONTROL MODULE block **190** notifies the control module **62** of the entry made by user **24**. In the manner similar to the login password, supra, the control module **62** queries the subscriber database and, at CONTROL MODULE RETRIEVES DTMF PASSWORD block **192**, retrieves the password or the generated password associated with the subscriber. At CONTROL MODULE VERIFIES DTMF PASSWORD block **194**, the control module **62** verifies that the password entered at the telephone keypad by the user matches the password retrieved from the subscriber database. Upon verification, the control module **62** at DOES THE DTMF PASSWORD MATCH? block **196** sends confirmation thereof back along the software pathway to inform the user of the event.

Upon failure to verify, the control module **62** at DOES THE DTMF PASSWORD MATCH? block **196** initiates an alarm indicating that the login conditions were not met. The software program upon an alarm condition terminates processing. As in the previous password verification and alternatively, the program offers the user an opportunity to retry. Whereupon there is a retracement through the same software path as just described and then, upon repeated alarm occurrence, the software program terminates processing. As before, the retry process may be limited to a specified number of times.

Upon out-of-band callback verification being received, the biometric identification portion of the software program is initiated. In this present embodiment, while the biometric parameter that is monitored is speech, any of a number of parameters may be used. In this case, the control module **62** instructs the speech module **66** at SPEECH MODULE RETRIEVES PROMPT FOR USER block **198** to retrieve a prompt that for the purpose of later playing the prompt to the user and collecting the speech password. The speech module **66** queries the announcement database **130** and retrieves the prompt to be played to the user **24**. Besides using a prepared prompt, as above, a prompt synthesized by the text-to-speech system **90**, **92** and **94** is utilizable for this purpose.

The prompt for collecting the speech password is played to the user **24** at PROMPT USER AND COLLECT SPEECH PASSWORD block **200**. The user **24**, who has previously had his biometric sample, namely the speech pattern, registered with the speech database **128**, the voices the speech password at USER VOICES SPEECH PASSWORD block **202** and transmits the same over the telephone at the remote computer **22** to the security computer **40**. Then, at SPEECH MODULE RETRIEVES SPEECH PASSWORD ASSOCIATED WITH LOGIN ID block **204**, the software program for the speech module **66** is adapted to query the speech database **128** and to retrieve the speech password associated with the accessor's login identification. Through the application of biometric analysis, such as voice recognition technology, the speech or module **66** at SPEECH MODULE VERIFIES SPEECH PASSWORD block **206** verifies that the voiced speech password received from the user **24** has the same pattern as the speech password retrieved from database **128**.

Upon verification, the speech module **66** at DOES THE SPEECH PASSWORD MATCH? block **208** sends confirmation thereof back along the software pathway to inform the user of the event. Upon failure to verify, the speech module **66** at DOES THE SPEECH PASSWORD MATCH? block **208** notifies the control module **62** which initiates an alarm indicating that the login conditions were not met. The software program upon an alarm condition terminates processing. As in the previous password verification and alternatively, the program offers the user an opportunity to retry. Whereupon there is a retracement through the same software path as just described and then, upon repeated alarm occurrence, the software program terminates processing.

As before, the retry process may be limited to a specified number of times. Upon being notified of a match between the pattern of the voiced speech password and that of the one retrieved from the database **128**, the control module **62** at CONTROL MODULE INSTRUCTS SPEECH MODULE TO ANNOUNCE ACCESS IS GRANTED block **210** instructs the speech module **66** to provide an announcement to the user **24** indicating that access is granted. The speech module **66** queries the announcement database **130** and retrieves the announcement for the user **24**. Alternatively, the announcement can be synthesized by the text-to-speech system **90**, **92** and **94** and played to the user **24**. Whichever announcement is used, it is made to the user at ACCESS GRANTED ANNOUNCEMENT MADE TO USER block **212**.

Upon completion of the announcement at SPEECH MODULE NOTIFIES CONTROL MODULE OF ANNOUNCEMENT block **214**, the speech module **66** notifies the control module **62** that the announcement has been made to the user **24**. At this point at DISCONNECT TELEPHONE CONNECTION WITH USER block **215**, the control module **62** instructs the line module **64** to terminate the telephone connection and the telephone connection between the security computer **40** and user **24** is severed. At CONTROL MODULE SENDS AUTHENTICATION MESSAGE TO SERVER PROTOCOL MODULE block **216**, the message that the user **24** is authenticated is relayed by control module **62** to server protocol module **116** which is requested to communicate the same to the client protocol module **114**.

At SERVER PROTOCOL MODULE SENDS AUTHENTICATION MESSAGE TO CLIENT PROTOCOL MODULE block **217**, the message is relayed to the client protocol module **114** and thence via a proprietary protocol, at CLIENT PROTOCOL MODULE SENDS AUTHENTICATION MESSAGE TO HOST COMPUTER block **218**, to the host computer **34**. The host computer or web server **34** at HOST COMPUTER GRANTS ACCESS TO USER block **219** grants access to the authenticated used **24**.

In FIG. **10** a schematic diagram of the second embodiment of the present invention is shown. For ease of comprehension, where similar components are used, reference designators "**200**" units higher are employed. In contrast to FIG. **1** which describes the out-of-band security networks for computer networks of this invention as applied to the internet or wide area networks, this embodiment describes the application to local area networks. The second embodiment is referred to generally by the reference designator **220**. Here the accessor is the computer equipment **222**, including the central processing unit and the operating system thereof, and the person or user **224** whose voice is transmittable by the telephone **226** over telephone lines **228**.

While in this example the biometric parameter monitored is voice patterns as interpreted by voice recognition systems, any of a number of other parameters may be used to identify the person seeking access. The access network **230** is constructed in such a manner that, when user **224** requests access to a high security database **232** located at a host computer **234** through computer **222**, the request-for-access is diverted by a router **236** internal to the corporate network **238** to an out-of-band security network **240**. Here the emphasis is upon right-to-know classifications within an organization rather than on avoiding entry by hackers.

Thus, as the accessor is already within the system, the first level of verification of login identification and password at the host computer is the least significant and the authentication of the person seeking access is the most significant. Authentication occurs in the out-of-band security network **240**, which is analogous to the one described in detail above, except the subscriber database becomes layered by virtue of the classification. This is in contradistinction to present authentication processes as the out-of-band security network **240** is isolated from the corporate network **238** and does not depend thereon for validating data. The overview shows the bibmetric validation which, in this case, takes the form of a voice network **242**.

In FIG. **11** a schematic diagram of the third embodiment of the present invention is shown. This embodiment describes the application of the security system to access over the internet. For ease of comprehension, where similar components are used, reference designators "**300**" units higher are employed. In contrast to FIG. **1** which describes the out-of-band security networks for computer networks of this invention as applied to wide area networks, this embodiment describes the application to internet networks. The third embodiment is referred to generally by the reference designator **320**. The case of user accessing a web application, such as an online banking application, (located on a web server **334**) over the internet **330**. The user from a computer **322** accesses the web application over an access channel and enters their USER ID. The web server **334** sends the USER ID to the security system **340**, also referred to as the centralized out-of-band authentication system (COBAS). COBAS **340** proceeds with authenticating the user through the user's cellular telephone over an authentication channel. The security system **340** calls the access-seeking user at the cellular telephone **326**. The user answers the phone and is prompted to enter a password for password verification and to enter a biometric identifier, such as a fingerprint. The security system **340** authenticates the user and sends the result to the web server **334**. Upon a positive authentication and after disconnecting from the authentication channel, access is granted along the access channel to the USER'S PC device **322**.

The flow diagram for the COBAS device **340** software is analogous to that described in the first embodiment, supra, but for the speech module **66**. In lieu thereof, in FIG. **12** the fingerprint module **366** architecture is detailed. The fingerprint verification hardware **384**, consists of digital signal processors that utilize algorithms for verification of an accessor's fingerprint. The fingerprint verification hardware **384** is controlled by the software program of the fingerprint hardware driver **386**. The software program of the fingerprint verification processing unit **388** provides an interface with control module **362** and is structured to respond to queries therefrom for verifying an accessor's password. Also, the fingerprint processing unit **388** enables the enrollment of users fingerprint and the interaction of the fingerprint database of the COBAS device **340**.

The text-to-speech (TTS) hardware **390** consists of digital signal processors that utilize TTS algorithms. The text-to-speech hardware **390** is controlled by the software program of the TTS hardware driver **392**. The software program of the TTS processing unit **394** provides an interface with the control module **362** and, as required by the control module **362**, converts text strings to synthesized speech. The announcement hardware **396** consists of digital signal processors that utilize speech algorithms to record and play announcements. The announcement hardware is controlled by the software program of the announcement hardware driver **398**. The software program of the announcement processing unit **400** also provides an interface with control module **362**; upon demands of the control module **362**, supplies stored announcements; and interacts with the announcements database of the related database (not shown).

In FIG. **13** a schematic diagram of the fourth embodiment of the present invention is shown. This embodiment describes the application to PDAs (Personal Digital Assistant). For ease of comprehension, where similar components are used, reference designators "**400**" units higher are employed. In contrast to FIG. **1** which describes the out-of-band security networks for computer networks as applied to wide area networks, this embodiment describes the application to wireless networks including peripherals, such as PDAs and cellular telephones. The fourth embodiment is referred to generally by the reference designator **420**.

Although there are several PDAs currently marketing including the Blackberry and the Palm Computer, in this embodiment an HP iPAQ running on a Windows CE operating system is utilized. These PDAs have wireless capabilities and can also incorporate custom software applications. The HP iPAQ hereof incorporates a fingerprint reader. The security system **420** has two distinct and independent channels of operation, namely, the access channel and the authentication channel. The user from a computer **422** accesses the web application over an access channel and enters their USER ID. The web server **434** sends the USER ID to the security system **440**. COBAS **440** proceeds with authenticating the customer via the wireless network **442** over an authentication channel.

The security system **440** sends an authentication request message to a software program located on the PDA **422**. The software program prompts the user to enter their fingerprint. The COBAS security system **440** now authenticates the user's fingerprint against the template stored in its database and send the result to the web server **434**. Upon a positive authentication and after disconnecting from the authentication channel, access is granted along the access channel to the USER'S PDA device **422**.

Because many varying and different embodiments may be made within the scope of the inventive concept herein taught, and because many modifications may be made in the embodiments herein detailed in accordance with the descriptive requirement of the law, it is to be understood that the details herein are to be interpreted as illustrative and not in a limiting sense.

What is claimed is:

1. A multichannel security system for accessing a host computer comprising:

an access channel comprising:

interception means for receiving and verifying a login identification originating from a demand from an accessor for access to said host computer; and

an authentication channel comprising:

a security computer for receiving from said interception means said demand for access together with said login identification and for communicating access information to said host computer and for communicating with a peripheral device of said accessor;

a database having at least one peripheral address record corresponding to said login identification;

prompt means for instructing said accessor to re-enter predetermined data at and retransmit predetermined data from said peripheral device; and

comparator means for authenticating access demands in response to the retransmission of said predetermined data by verifying a match between said predetermined data and said re-entered and retransmitted data,

wherein said security computer outputs an instruction to the host computer to either grant access thereto using said access channel or to deny access thereto.

2. A multichannel security system as described in claim **1** wherein:

said peripheral device is a telephone with a tone generating keypad for entering data; and,

said prompt means is an auditory message describing data to be entered.

3. A multichannel security system as described in claim **2** wherein said security computer further comprises:

an announcement database; and

a voice module for selecting a prerecorded auditory message from said announcement database and, for prompting the entry of data by said accessor, playing said prerecorded auditory message over said telephone.

4. A multichannel security system as described in claim **3** wherein upon outputting an instruction to the host computer to grant access, said security computer communicates in said authentication channel the access information to said accessor by selecting and transmitting an access-granted message from said announcement database and sequentially disconnecting from the connection with said telephone prior to use of said access channel.

5. A multichannel security system as described in claim **2** wherein said authentication channel further comprises:

a voice module, capable of synthesizing an auditory message, and, for prompting the entry of data by said accessor, playing a synthesized auditory message over said telephone.

6. A multichannel security system as described in claim **5** further comprising:

an announcement database, wherein upon outputting an instruction to the host computer to grant access, said security computer communicates in said authentication channel the access information to said accessor by selecting and transmitting an access-granted message from said announcement database and sequentially disconnecting from the connection with said telephone prior to use of said access channel.

7. A multichannel security system as described in claim 1 wherein said security computer further comprises:

authentication program means for authenticating access to said host computer;

a biometric analyzer operating in response to instructions from said authentication program means for analyzing a monitored parameter of said accessor; and,

a biometric parameter database addressable by said biometric analyzer for retrieval of a previously registered sample of said accessor, said sample corresponding to the identification of said accessor.

8. A multichannel security system as described in claim 7 wherein said biometric analyzer is a voice recognition program for operation within said authentication channel.

9. A multichannel security system as described in claim 8 wherein said voice recognition program comprises:

a speech database for retrieval of a speech sample of said accessor corresponding to said login identification;

said security computer adapted to provide instructions to connect and disconnect said security computer to and from said peripheral device;

voice sampling means for instructing said accessor to repeat back and transmit a predetermined auditory statement over said peripheral device;

voice recognition means for authenticating at least one access demands in response to transmission of said predetermined auditory statement; and,

said security computer, upon authenticating a match between the predetermined auditory statement and the transmitted voice data and upon disconnecting from said authentication channel, providing authentication of the accessor and instructing the host computer to grant access along said access channel.

10. A multichannel security system as described in claim 7 wherein said biometric analyzer comprises a fingerprint verification program.

11. A multichannel security system for granting and denying access to a host computer, said access in response to a demand from an accessor for access to the host computer, said accessor having a cellular telephone for providing communications to the security system, said multichannel security system comprising:

a login identification accompanying said demand from said accessor;

interception means for receiving and verifying said login identification, said interception means in an access channel;

an authentication channel operating independently from said access channel, said authentication channel comprising:

a security computer adapted in an access-channel mode to receive from said interception means said demand for access together with said login identification and to communicate access information to said host computer and in an authentication-channel mode communications with said cellular telephone;

a subscriber database for retrieval of peripheral addresses corresponding to said login identification;

wherein said security computer is adapted to connect to said associated cellular telephone of said accessor;

prompt means for instructing said accessor to re-enter predetermined data at and retransmit predetermined data from said cellular telephone;

comparator means for authenticating access demands in response to retransmission of predetermined data from said cellular telephone;

said security computer, upon verifying a match between said predetermined data and said re-entered and retransmitted data, providing in the access-channel mode instructions to the host computer to grant access thereto along said access channel;

authentication program means, operating independently from said host computer, for authenticating said accessor demanding access to said host computer;

a biometric analyzer operating in response to said instructions from said authentication program means to analyze a monitored parameter of said accessor; and,

a biometric parameter database addressable by said biometric analyzer for retrieval of a previously registered sample of said accessor, said sample corresponding to the identification of said accessor.

12. A multichannel security system as described in claim 11 wherein said security computer further comprises:

an announcement database; and

a voice module capable of selecting a prerecorded auditory message from said announcement database and for prompting the entry of data by said accessor, playing said prerecorded auditory message over said telephone.

13. A multichannel security system as described in claim 12 wherein, upon attaining an access-granted condition, said security computer communicates in said authentication channel the access information to said accessor by selecting and transmitting an access-granted message from said announcement database and sequentially disconnecting from the connection with said telephone prior to use of said access channel.

14. A multichannel security system as described in claim 11 wherein said authentication channel further comprises:

a voice module capable of synthesizing an auditory message, and, for prompting the entry of data by said accessor, playing a synthesized auditory message over said telephone.

15. A multichannel security system as described in claim 11 wherein said biometric analyzer comprises a voice recognition program for operation within said authentication channel to authenticate said accessor.

16. A multichannel security system as described in claim 15 wherein said voice recognition program comprises:

a speech database for retrieval of a speech sample of said accessor corresponding to the login identification of said accessor;

said security computer adapted to provide instructions to connect and disconnect said security computer to and from said cellular telephone;

voice sampling means for instructing said accessor to repeat back and transmit a predetermined auditory statement over said cellular telephone to said security computer;

voice recognition means in said security computer for authenticating access demands in response to transmission of said predetermined auditory statement received over said cellular telephone; and,

wherein said security computer, upon authenticating a match between the predetermined auditory statement and the transmitted voice data and upon disconnecting from said authentication channel, providing authentication of said accessor and instructing the host computer to grant access along said access channel.

17. A multichannel security system as described in claim 11 wherein said biometric analyzer comprises a fingerprint verification program for operation within said authentication channel to authenticate said accessor.

18. A multichannel security system for granting and denying access to a host computer, said access in response to a demand over the Internet from an accessor for access to the host computer, said accessor having a personal digital assistant (PDA) for providing communications to the security system, said multichannel security system comprising:

a login identification accompanying said demand over the internet from said accessor;

interception means for receiving and verifying said login identification, said interception means in an access channel;

an authentication channel operating independently from said access channel and, said authentication channel, in turn, comprising;

a security computer adapted in an access-channel mode to receive from said interception means said demand together with said login identification and to communicate access information to said host computer and in an authentication-channel mode communications with said PDA;

a subscriber database for retrieval of peripheral addresses corresponding to said login identification;

said security computer adapted to connect to said PDA;

prompt means for instructing said accessor to re-enter predetermined data at and retransmit predetermined data from said PDA;

comparator means for authenticating access demands in response to retransmission of predetermined data from said PDA;

said security computer, upon verifying a match between said predetermined data and the re-entered and retransmitted data, providing in the access-channel mode instructions to the host computer to grant access thereto along said access channel;

authentication program means, operating independently from said host computer, for authenticating an accessor demanding access to said host computer;

a biometric analyzer operating in response to instructions from said authentication program means to analyze a monitored parameter of said accessor; and,

a biometric parameter database addressable by said biometric analyzer for retrieval of a previously registered sample of said accessor, said sample corresponding to the identification of said accessor.

19. A multichannel security system as described in claim 18 wherein said biometric analyzer comprises a fingerprint verification program for operation within said authentication channel to authenticate the accessor.

20. A multichannel security system as described in claim 19 wherein, upon attaining an access-granted condition, said security computer communicates in said authentication channel the access information to said accessor by selecting and transmitting an access-granted message from said announcement database and sequentially disconnecting from the connection with said telephone prior to use of said access channel.

21. A method for accessing a host computer comprising the steps of:

in an access channel, receiving at a control module a login identification from an accessor;

in an authentication channel that is separate from the access channel:

providing a security computer comprising a subscriber database, the database having at least one peripheral address of a peripheral device;

receiving in the security computer an intercepted login identification corresponding to the login identification;

retrieving a peripheral address corresponding to the intercepted login identification;

outputting to the peripheral address a first instruction to re-enter predetermined data at and retransmit the predetermined data from the peripheral device;

comparing at the security computer the re-entered and retransmitted data; and

outputting a second instruction to the host computer to either grant access thereto using the access channel or to deny access thereto.

22. The method according to claim 21, wherein the peripheral device is one of a telephone, a cellular telephone, and a PDA each having an input device for entering data.

23. The method according to claim 21, wherein the outputted first instruction comprises an auditory message describing data to be entered.

24. The method according to claim 21, wherein the security computer further comprises an announcement database.

25. The method according to claim 24, further comprising the steps of:

selecting a prerecorded auditory message from the announcement database; and

outputting the prerecorded auditory message at the peripheral device.

26. The method according to claim 25, further comprising the steps of:

at said security computer and after outputting the second instruction, communicating in the authentication channel the access information to the accessor by selecting and transmitting an access-granted message from the announcement database; and

disconnecting from the connection with the peripheral device prior to use of the access channel.

27. The method according to claim 21, wherein the authentication channel further comprises a voice module for requesting the entry of data at the peripheral device by outputting a synthesized auditory message at the peripheral device.

28. The method according to claim 21, further comprising the steps of:

providing in the authentication channel a biometric analyzer for analyzing a monitored parameter of the accessor;

providing a biometric parameter database addressable by the biometric analyzer for retrieval of a previously registered sample of the accessor, the sample corresponding to the identification of the accessor; and,

authenticating access to the host computer using the biometric analyzer.

29. The method according to claim 28, wherein the biometric analyzer comprises a voice recognition device.

30. The method according to claim 29, wherein the voice recognition program comprises:

a speech database for retrieval of a speech sample of the accessor corresponding to the intercepted login identification;

voice sampling means for instructing the accessor to repeat back and transmit a predetermined auditory statement over the peripheral device; and

voice recognition means for authenticating at least one access demand in response to transmission of the predetermined auditory statement.

31. The method according to claim 28, wherein the biometric analyzer comprises a fingerprint verification device.

32. An out-of-band computer security system comprising:

a security computer in an authentication channel for communicating with a telephonic device and for receiving an intercepted demand for access to a host computer together with a login identification from an accessor in an access channel that is separate from the authentication channel;

a subscriber database addressable by the security computer having at least one telephone number corresponding to the intercepted login identification;

a device operable in response to a first instruction from the security computer to call the at least one telephone number and connect the telephonic device to the security computer;

prompt means for outputting a second instruction at the telephonic device to re-enter predetermined data at and retransmit predetermined data from the telephonic device; and

comparator means in said security computer for authenticating the access demand in response to the retransmission of the predetermined data from the telephonic device;

wherein the security computer, upon verifying a match between the predetermined data and the re-entered and retransmitted data, authenticates the accessor and instructs the host computer to grant access thereto in the access channel.

33. An out-of-band security system as described in claim 32, further comprising:

a biometric analyzer for analyzing a monitored parameter of the accessor;

a biometric parameter database addressable by the biometric analyzer for retrieval of a previously registered sample of the accessor, the sample corresponding to the identification of the accessor;

sampling means for instructing the accessor to provide and transmit a predetermined entry of the monitored parameter using the telephonic device; and

second comparator means for providing authentication to the security computer in response to a matching analysis between the characteristics of the sample and of the transmission of the predetermined entry of the accessor,

wherein the security computer, upon verifying a match between the predetermined entry and the sample, authenticates the accessor and instructs the host computer to grant access thereto in the access channel.

34. An out-of-band security system as described in claim 32, further comprising:

an auditory message prompting the accessor to enter predetermined data at and retransmit predetermined data from the telephonic device; and

second comparator means for authenticating the access demand in response to retransmission of predetermined data from the telephonic device,

wherein the security computer, upon verifying a match between the predetermined data and the entered and retransmitted data, authenticates the accessor and instructs the host computer to grant access thereto in the access channel.

* * * * *

US007870599C1

(12) EX PARTE REEXAMINATION CERTIFICATE (8779th)

United States Patent
Pemmaraju

(10) **Number: US 7,870,599 C1**
(45) **Certificate Issued: Dec. 27, 2011**

(54) **MULTICHANNEL DEVICE UTILIZING A CENTRALIZED OUT-OF-BAND AUTHENTICATION SYSTEM (COBAS)**

(75) Inventor: **Ram Pemmaraju**, Old Bridge, NJ (US)

(73) Assignee: **Netlabs.com Inc.**, Edison, NJ (US)

Reexamination Request:
No. 90/011,429, Jan. 11, 2011

Reexamination Certificate for:

Patent No.:	**7,870,599**
Issued:	**Jan. 11, 2011**
Appl. No.:	**10/970,559**
Filed:	**Oct. 21, 2004**

Related U.S. Application Data

(63) Continuation-in-part of application No. 09/655,297, filed on Sep. 5, 2000, now abandoned.

(51) **Int. Cl.**

G06F 7/04	(2006.01)
G06F 21/00	(2006.01)
H04L 29/06	(2006.01)

(52) **U.S. Cl.** 726/2; 726/4; 713/168; 713/169; 713/186; 340/5.8; 340/5.81; 340/5.82; 340/5.83; 340/5.84

(58) **Field of Classification Search** 726/5
See application file for complete search history.

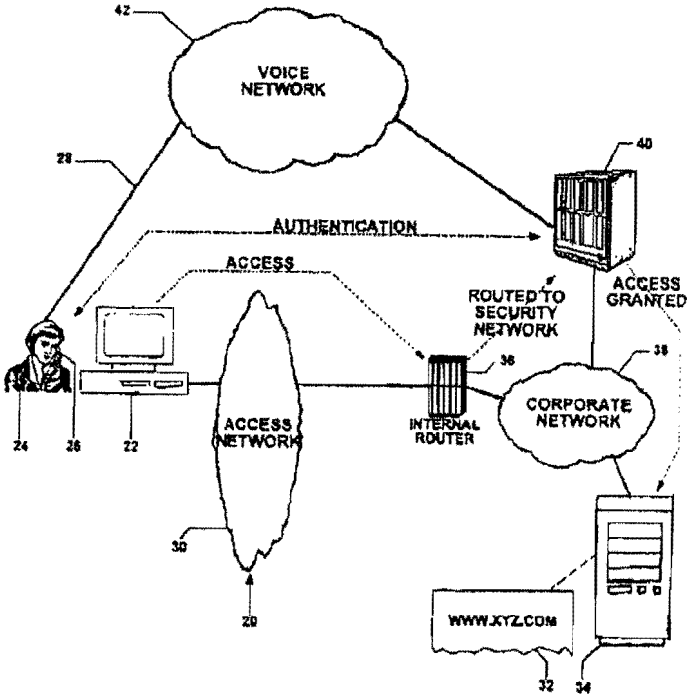
(56) **References Cited**

To view the complete listing of prior art documents cited during the proceeding for Reexamination Control Number 90/011,429, please refer to the USPTO's public Patent Application Information Retrieval (PAIR) system under the Display References tab.

Primary Examiner—Minh Dieu Nguyen

(57) **ABSTRACT**

A multichannel security system is disclosed, which system is for granting and denying access to a host computer in response to a demand from an access-seeking individual and computer. The access-seeker has a peripheral device operative within an authentication channel to communicate with the security system. The access-seeker initially presents identification and password data over an access channel which is intercepted and transmitted to the security computer. The security computer then communicates with the access-seeker. A biometric analyzer—a voice or fingerprint recognition device—operates upon instructions from the authentication program to analyze the monitored parameter of the individual. In the security computer, a comparator matches the biometric sample with stored data, and, upon obtaining a match, provides authentication. The security computer instructs the host computer to grant access and communicates the same to the access-seeker, whereupon access is initiated over the access channel.



EX PARTE REEXAMINATION CERTIFICATE ISSUED UNDER 35 U.S.C. 307

THE PATENT IS HEREBY AMENDED AS INDICATED BELOW.

Matter enclosed in heavy brackets [ ] appeared in the patent, but has been deleted and is no longer a part of the patent; matter printed in italics indicates additions made to the patent.

AS A RESULT OF REEXAMINATION, IT HAS BEEN DETERMINED THAT:

The patentability of claims **1-34** is confirmed.

New claims **35-42** are added and determined to be patentable.

35. A multichannel security system as described in claim 1 wherein said predetermined data is a DTMF password.

36. A multichannel security system as described in claim 35 wherein said DTMF password is a numeric fixed sequence of numbers or non-numeric key on a telephone keypad.

37. A multichannel security system as described in claim 1 wherein said predetermined data is prompted using an application on the peripheral device.

38. A multichannel security system as described in claim 1 wherein said predetermined data is prompted using an application on the access computer.

39. A multichannel security system as described in claim 1 wherein said instruction to said accessor to re-enter predetermined data is an announcement stored in an announcement database and played to the accessor.

40. A multichannel security system as described in claim 39 wherein the announcement is recorded speech.

41. A multichannel security system as described in claim 39 wherein the announcement is a generated password relayed to the accesor

42. A multichannel security system as described in claim 7 wherein said biometric analyzer is a facial recognition program for operation within said authentication channel.

* * * * *

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS
StrikeForce Technologies, Inc.

DEFENDANTS
PhoneFactor, Inc., Fiserv, Inc., First Midwest Bancorp. Inc.

(b) County of Residence of First Listed Plaintiff Middlesex County, NJ
(EXCEPT IN U.S. PLAINTIFF CASES)

County of Residence of First Listed Defendant Johnson County, KS
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Steven L. Caponi, Esq. Blank Rome LLP, 1201 Market Street, Suite 800
Wilmington, DE 19801 (302) 425-6408

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☒ 830 Patent
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS - Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation

VI. CAUSE OF ACTION
Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
35 U.S. C. Section 271
Brief description of cause:
Patent Infringement

VII. REQUESTED IN COMPLAINT: ☐ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P. **DEMAND $** CHECK YES only if demanded in complaint: **JURY DEMAND:** ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY *(See instructions)*: JUDGE _____ DOCKET NUMBER _____

DATE 03/28/2013

SIGNATURE OF ATTORNEY OF RECORD /s/Steven L. Caponi (DE ID. No. 3484)

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

V. Origin. Place an "X" in one of the six boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407. When this box is checked, do not check (5) above.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.