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

(54) Title: METHOD AND SYSTEM FOR AUTHENTICATING INTERNET USER INDENTITY
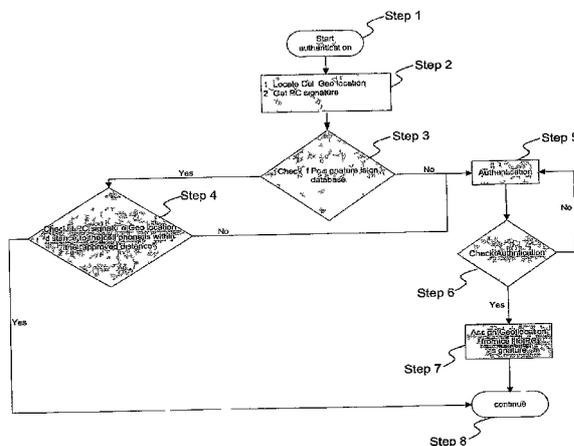
FIG 1

(57) **Abstract:** A method and system for authenticating an Internet user identity by cross-referencing and comparing at least two independent sources of information. A first geographical location of computer signature of an internet user is identified and the geographical location of a communication voice device of said internet user is identified to determine a second location. The first and second locations are compared for geographical proximity to confirm the identity of the internet user. Based upon geographical proximity of said locations, a score is assigned to the internet user, and access to a website is allowed or limited based upon said score. Alternatively, additional authentication information can be required or access can be terminated.

TITLE: METHOD AND SYSTEM FOR AUTHENTICATING INTERNET USER
       IDENTITY
INVENTOR: GUY s. HEFFEZ

PATENT APPLICATION

CROSS-REFEERENCE TO RELATED APPLICATIONS

   None.

TECHNICAL FIELD

     This invention relates to internet user
identification. More specifically it relates to using computer
characteristics to identify an internet user. Even more
specifically it relates to using characteristics of the user's
computer and a cell phone location to identify the user.

BACKGROUND ART

    The invention relates to a method and system for
authenticating internet user identity, and more particularly,
to a method and system for authenticating internet user

identity by cross-referencing the geographical location of a
internet user's Communication voice device, such as a mobile
voice device, a Voice over Internet Protocol (hereinafter
VoIP) telephone or non-mobile telephone, and the geographical
5   location of the computer signature.

      Computer signature can be set of one or more hardware
devices information, unlimited example the gateway Mac
address, the computer Mac address, CPU serial number and more.
10   The computer signature can also be set of one or more software
components. Unlimited example – the operating system serial
number, cookie, combination of few software's versions etc'
hereinafter (computer signature)

15   The use of the internet has become a common a popular
arena for the sale of goods and services. Such sales require
the transmission of personal and confidential data belonging
to the buyer of such goods and services. Such information is
often the target of identity theft. In response to the
20   increase in the opportunity for the commission of fraud
through identity theft, sellers and providers of goods and
services through the internet require a method whereby such
fraud can be reduced.

25   With respect to internet usage, upon accessing the
internet, an internet user's computer is identified with an IP
address, it should be understood that Internet Protocol
Address (hereinafter "IP Address") means any internet
communication protocol such as but not limited to IPV4 and
30   IPV6. And whenever the internet user enters a website, the
internet user's IP address is identified to the website owner.
Such identified IP addresses can be traceable geographically

to its source so as to determine the location (state and city)
of the internet user, in some cases the IP address can be
traced to a radius of a few miles from its source. The
comparison of the geographical location of the internet user
computer signature, with the geographical location of said
internet user Communication voice device can provide the
seller or provider a means to authenticate the identify of the
internet user.

United States Pat. App. Pub. No. 2001/0034718 Al to
Shaked et al. discloses a method of controlling access to a
service over a network, including the steps of automatically
identifying a service user and acquiring user information,
thereby to control access. Additionally, a method of
providing service over a network, in which the service
requires identification of a user, including the steps of
automatically identifying the user and associating the user
with user information, thus enabling the service, is
disclosed.

United States Pat. No. 6,466,779 to Moles et al.
discloses a security apparatus for use in a wireless network
including base stations communicating with mobile stations for
preventing unprovisioned mobile stations from accessing an
internet protocol (IP) data network via the wireless network.

United States Pat. App. Pub. No. 2002/0188712 Al to
Caslin et al. discloses a fraud monitoring system for a
communications system. The fraud monitoring system analyzes
records of usage activity in the system and applies fraud
pattern detection algorithms to detect patterns indicative of
fraud. The fraud monitoring system accommodates both

transaction records resulting from control of a packet-switched network and those from a circuit-switched network gateway.

5   United States Pat. App. Pub. No. 2003/0056096 Al to Albert et al. discloses a method to securely authenticate user credentials. The method includes encrypting a user credential with a public key at an access device. The public key is part of a public/private key pair suitable for use with encryption
10   algorithm. The decrypted user credential is then transmitted from the decryption server to an authentication server for verification. The decryption server typically forms part of a multi-party service access environment including a plurality of access providers. This method can be used in legacy
15   protocols, such as Point-to-Point Protocol (PPP), Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), Remote Authentication Dial in User Server (RADIUS) protocol, Terminal Access Controller Access Control System (TACAS) protocol, Lightweight Directory
20   Access Protocol (LDAP), NT Domain authentication protocol, Unix password authentication protocol, Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol over Secure sockets layer (HTTPS), Extended Authentication Protocol (EAP), Transport Layer Security (TLS) protocol, Token Ring protocol,
25   and/or Secure Remote Password protocol (SRP).

        United States Patent Application Publication Number US 2003/0101134 Al published to Liu et *al.* on May 29, 2003 teaches a method for transaction approval, including
30   submitting a transaction approval request from a transaction site to a clearing agency; submitting a user authorization request from the clearing agency to a user device; receiving a

response to the user authorization request; and sending a
response to the transaction approval request from the clearing
agency to the transaction site. Another method for
transaction approval includes: submitting a transaction
approval request from a transaction site to a clearing agency;
determining whether a trusted transaction is elected;
submitting a user authorization request from the clearing
agency to a user device if a trusted transaction is determined
to be elected; receiving a response to the user authorization
request from the user device if the user authentication
request was submitted; and sending a response to the
transaction approval request from the clearing agency to the
transaction site. A system for transaction approval includes
a clearing agency for the transaction approval wherein the
clearing agency having a function to request for user
authorization, a network operatively coupled to the clearing
agency, and a user device adapted to be operatively coupled to
the network for trusted transaction approval .

United States Patent Application Publication Number US
2003/0187800 Al published to Moore et *al.* on October 2, 2003
teaches systems, methods, and program products for determining
billable usage of a communications system wherein services are
provided via instant communications. In some embodiments,
there is provided for authorizing the fulfillment of service
requests based upon information pertaining to a billable
account .

United States Patent Application Publication Number US
2004/0111640 Al published to Baum on June 10, 2004 teaches
methods and apparatus for determining, in a reliable manner, a
port, physical location, and/or device identifier, such as a

MAC address, associated with a device using an IP address and
for using such information, *e.g.,* to support one or more
security applications. Supported security applications
include restricting access to services based on the location
of a device seeking access to a service, determining the
location of stolen devices, and authenticating the location of
the source of a message or other IP signal, e.g., to determine
if a prisoner is contacting a monitoring service from a
predetermined location.

United States Patent Application Publication Number US
2005/0159173 Al published to Dowling on July 21, 2005 teaches
methods, apparatus, and business techniques for use in mobile
network communication systems. A mobile unit, such as a smart
phone, is preferably equipped with a wireless local area
network connection and a wireless wide area network
connection. The local area network connection is used to
establish a position-dependent, e-commerce network connection
with a wireless peripheral supplied by a vendor. The mobile
unit is then temporarily augmented with the added peripheral
services supplied by the negotiated wireless peripheral.
Systems and methods allow the mobile unit to communicate
securely with a remote server, even when the negotiated
wireless peripheral is not fully trusted. Also included are
mobile units, wireless user peripherals, and negotiated
wireless peripherals projecting a non-area constrained user
interface image on a display surface.

United States Patent Application Publication Number US
2005/0160280 Al published to Caslin *et al.* on July 21, 2005
teaches providing fraud detection in support of data
communication services. A usage pattern associated with a

particular account for remote access to a data network is
monitored. The usage pattern is compared with a reference
pattern specified for the account. A fraud alert is
selectively generated based on the comparison.

5

United States Patent Application Publication Number US
2005/0180395 Al published to Moore et *al.* on August 18, 2005
teaches an approach for supporting a plurality of
communication modes through universal identification. A core

10 identifier is generated for uniquely identifying a user among
a plurality of users within the communication system. One or
more specific identifiers are derived based upon the core
identifier. The specific identifiers serve as addressing
information to the respective communication modes. The

15 specific identifiers and the core identifier are designated as
a suite of identifiers allocated to the user.

While these systems may be suitable for the particular
purpose employed, or for general use, they would not be as

20 suitable for the purposes of the present invention as
disclosed hereafter.

DISCLOSURE OF THE INVENTION

It is an object of the invention to produce a means to decrease the potential for fraud through authentication of the identity of an internet user. Accordingly, this method provides for authenticating the identity of the internet user or purchaser (hereinafter "internet user") through cross-referencing and comparison of at least two independent sources of information, such as, but not limited to, the internet user's computer signature geographical location and the geographical location of a Communication voice device associated with said internet user.

It is another object of the invention to provide a means for providing an accurate geographical location of the internet user and the internet user's computer signature.

It is another object of the invention to provide a convenient means for determining the location of internet users at both mobile and non-mobile Communication voice devices and terminals. Accordingly, this method includes the utilization systems and software that are used to locate the geographical location of people or Communication voice devices, such as, but not limited to Global Positioning Systems (GPS), Galileo, WiMax, WiFi, RFID and external positioning apparatus, such as, but not limited to, cellular base stations and antennas.

It is another object of the invention to provide a convenient means for determining a more accurate geographical location of routers using the internet user Communication

voice device's geographical location and the said user computer signature.

This invention is a method and system for authenticating an internet user identity by cross-referencing and comparing at least two independent sources of information. A first computer signature of an internet user is identified. The geographical address of a communications device of said internet user is traced to determine a second location. The first and second locations are compared for geographical proximity to confirm the identity of the internet user. Additionally, depending on the geographical proximity of the first and second location, a positive or negative score may be assigned to the internet user, and access to the website and the ability to conduct transactions may be allowed or limited based on the assigned score. Alternatively, additional authentication information may be required of the internet user in order to proceed with the online transaction, or access by the internet user may be terminated.

A computer signature is created by identifying certain characteristics of the computer. These characteristics act as identifiers of the computer. Every computer that is connected to the internet has few unique identifiers such as but not limited to: Computer Network Mac address, CPU serial number, Operating System S/N. and more. In addition to the above the computer uses other network resources that have unique identifiers such as but not limited to a Gateway or Router Mac Address. In addition to the above every computer has common identifiers such as but not limited to: Operating system version, Disk Size, Internet browser version, hardware installed on the computer, network card speed, Operating

system patches installed on the computer, CPU speed, memory size, cookie, secret cookie, virtual memory size, other installed software on the computer and more. Using one or more then one common identifiers together it is possible to create 5   one unique computer signature for any given computer.

To the accomplishment of the above and related objects the invention may be embodied in the form illustrated in the accompanying drawings. Attention is called to the fact, 10   however, that the drawings are illustrative only. Variations are contemplated as being part of the invention, limited only by the scope of the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

In the drawings, like elements are depicted by like
reference numerals.   The drawings are briefly described as
5   follows .

FIG 1 is a flow chart of the method and system of the
present invention.

10   BEST MODE FOR CARRYING .OUT THE INVENTION

This invention relates to a method and system for
authenticating internet user identity by cross-referencing or
comparing at least two independent sources of information,
15   identifying at least two geographical locations. Based upon
geographical proximity of said locations, a score is assigned
to the internet user, and predetermined access to a website
and an ability to conduct transactions is allowed or limited
based upon said score. Alternatively, additional
20   authentication information can be required or access can be
terminated.   The invention is also a convenient means for
determining a more accurate geographical location of routers.

FIG 1 illustrates a method for authenticating internet
25   user identity by cross-referencing and comparing at least two
independent sources of information. In step 1, an internet
user starts authentication. Then, in step 2, the online entity
locates the geographic location of the internet user's cell
phone and checks the user's computer signature. In step 3, the
30   online entity looks for the computer signature in a database.
If the computer signature is discovered, the method proceeds
to step 4. In step 4, the online entity compares the distance

between the geographic location of the computer defined by the computer signature and the geographic location of the user's cell phone. If the distance is acceptable, the authentication process continues at step 8. If the distance is not

5   acceptable, the method goes to step 5.

If the computer signature is not in the database, the method also continues to step 5. In step 5, the online entity attempts to authenticate the computer by other means. In step

10   6, the authentication is confirmed. If the authentication is acceptable, the method continues to step 7. If the authentication is not acceptable, the method returns to step 5 and repeats step 5.

15   If the authentication is acceptable, continues to step 7 assigning the geographic location of the user's cell phone to the computer signature and saving it in the database. The method then continues with the authentication in step 8.

20   Referring to Fig 1, the method starts when the online entity decides to authenticate the internet user accessing a website and provides information, as in steps 1 and 2. The website vendor then decides to authenticate internet user identity, based on the information provided by the internet

25   user, as shown in step 3. What information will trigger the decision to authenticate the identity of the internet user will vary among vendors employing the method described herein. For purposes of clarity, the term vendor will be used hereafter and it should be understood that vendor means any

30   business, organization or commercial entity which conducts on-line commercial transactions through a website on the internet, such as, but not limited to, banking institutions,

on-line stores or other commercial or none commercial entities .

Upon accessing a website, in step 2, the computer signature will be identified. The invention is not limited to a conventional computer, but may include terminals, smart phones (PDA's) or other devices capable of communicating with the internet. Whenever the internet user enters a website, the internet user's computer signature is identified for a website owner.

A computer signature is created by identifying certain characteristics of the computer. These characteristics act as identifiers of the computer. Every computer that connected to the Internet has few unique identifiers. Using one, or more then one, common identifiers together it is possible to create one unique computer signature. These identifiers are selected from the list of Computer Network Mac address, CPU serial number, Operating System S/N. and more. In addition to the above the computer uses other network resources that have unique identifiers such as but not limited to a Gateway or Router Mac Address. In addition to the above every computer has common identifiers such as but not limited to: Operating system version, Disk Size, Internet browser version, hardware installed on the computer, network card speed, Operating system patches installed on the computer, CPU speed, memory size, virtual memory size, other installed software on the computer and more. A person skilled in the art will see that other computer characteristics could be used as identifiers to create a computer signature.

The vendor will then request from the internet user a contact number for a communications voice device, which is accessible to the internet user at the internet user's current location. Communication voice device, as used in the context

5   of the present invention, applies to any voice device capable of communicating with another voice device such as, but not limited to, phone, mobile voice device, VoIP telephone or personal digital assistant (hereinafter PDA). Other non-limiting examples include any device that has been modified or

10   designed for voice or text communication. A geographical location for the communication voice device is then traced, as stated in step 2.

It should be understood that the term "mobile voice

15   device", as used in the context of the present invention, applies to any mobile device modified or designed for voice or text communication and capable of communicating with another device via wireless network such as but not limited to cellular system, radio system, WiFi, WiMax, RFID, Bluetooth,

20   MIMO, UWB (Ultra Wide Band), satellite system or any other such wireless networks known now or in the future.

Other non-limiting examples include any device that has been modified or designed to communicate with a web-ready PDA,

25   a Blackberry, a laptop computer with cellular connect capability, or a notification server, such as email server.

The geographical location of a telephone can be traced using any one of existing databases. As a non-mobile telephone

30   is attached to a single physical location, the location is available using various existing databases. A Voice over Internet Protocol (hereinafter VoIP) telephone is connected to

high-speed internet access such as Tl, DSL, cable modems, or other available internet connection systems. A VoIP location is available using various databases. A VoIP connection provider company can provide the IP address to which such VoIP telephone is connected such that the geographical location of the internet user is traceable to the IP address.

The geographical location of a mobile voice device can be traced using technology such as, but not limited to, Galileo, GPS, cellular antenna network, phone antenna, WiFi, Bluetooth, MIMO, UWB, WiMax, etc.

A cellular telephone location system for automatically recording the location of one or more mobile cellular telephones is described, for example, in U.S. Pat. No. 5327144. The system comprises a central site system operatively coupled to at least three cell sites. Each of the cell sites receives cellular telephone signals and integrates a timing signal common to all the cell sites. The central site calculates differences in times of arrival of the cellular telephone signals arriving among the cell sites and thereby calculates the position of the cellular telephone producing the cellular telephone signals. Additional examples of known methods for locating phones are cell sector and cell site.

The position of an internet user's mobile voice device can be determined by, for example: (a) an internal positioning apparatus such as a Global Positioning System (hereinafter GPS) receiver built into the mobile voice device that receives GPS radio signals transmitted from GPS satellites; and (b) an external positioning apparatus such as a cellular positioning system that computes the position of the mobile voice device

15   .

by observing time differences among the arrivals of a radio signal transmitted by the mobile voice device at a plurality of observation points, i.e., base stations. The operation of the GPS is well-known and will not be described further
5. herein.

Next, the geographical location of the IP address of the internet user is traced, as stated in step 2. Such an IP address can be traced geographically to its source so as to
10 determine the location (state and city) of the internet user. In some cases the system used to trace the IP address can be so accurate that it can identify a street and house number of the internet user.

15   Another means for obtaining the geographical location of the internet user's computer signature, the internet user's ISP can be contacted to request a full address from where the internet user is connected. For example, a modem dial-up internet user is assigned a unique computer signature by their
20 ISP. After the internet user enters a username and password the ISP knows from which phone number that internet user called and can trace a contacting number to a geographical location.

25   The present invention includes a method of locating a router's geographical location based on the computer signature geographical location. In addition, the invention includes a method of geographically comparing the user communication voice device and the computer signature. All of the methods
30 may utilize a communication voice device that is either non-mobile telephone, a mobile telephone or a mobile voice device.

Since the following is known:
1.   The geographical location of the user's computer
        signature.
2.   The routing table between the vendor internet web
        site and the internet user.

Then, the vendor can locate the geographical location of the
closest public router to the internet user computer signature.
Since the first public router that the internet user is using
is close geographically to the internet user computer
signature.

It is to be understood that the present invention is not
limited to the embodiments described above, but encompasses
any and all embodiments under the doctrine of equivalents.

In conclusion, herein is presented a method and system
for authenticating internet user identity. The invention is
illustrated by example in the drawing figures, and throughout
the written description. It should be understood that
numerous variations are possible, while adhering to the
inventive concept. Such variations are contemplated as being
a part of the present invention.

INDUSTRIAL APPLICABILITY

This invention can be used for any purpose that is
related to internet security, internet commerce and internet
user identification. The invention is specifically envisioned
as an improvement over existing log-in methods and purchases
identification methods, but a person skilled in the art will
recognize other applications.

CLAIMS

What is claimed is:

5   1. A method of authenticating internet user identity,
       comprising the steps of:

           a) Creating a computer signature by identifying a
       specific computer with one or more qualities of the
10   computer;

           b) Identifying a Computer signature of the internet
       user;

15   c) Requesting a number for a communication voice
       device of said internet user;

           d) Determining a current geographical location of
       said communication voice device of said internet user;
20
           e) Tracing a geographical location of the Computer
       signature of the internet user; and

           f) Comparing the geographical location of the
25   Computer signature with the geographical location of the
       communication voice device of said internet user.

       2. The method of claim 1 where the computer signature is
       created from one or more qualities selected from the
30   following list: Computer Network Mac address, CPU serial
       number, Operating System S/N, Gateway Mac Address, operating
       system version, Router Mac Address, disk size, internet

browser version, hardware installed on the computer, network card speed, operating system patches, CPU speed, memory size, virtual memory size, and software installed on the computer.

5

3. The method of claim 1, further comprising the step of determining if a result obtained by comparing the geographical location of the Computer signature of the internet user with the geographical location of the

10   communication voice device of the internet user is within a predetermined distance value.

4. The method of claim 1, wherein the communication voice device is a non-mobile telephone.

15

5. The method of claim 1, wherein the communication voice device is a mobile telephone.

6. The method of claim 1, wherein the communication voice

20   device is a mobile voice device

7. A method of locating a router's geographical location based on an internet user communication voice device's geographical location and internet user Computer signature.

25

8. The method of claim 7, wherein the communication voice device is a non-mobile telephone.

9. The method of claim 7, wherein the communication voice

30   device is a mobile telephone.

.

10. The method of claim 7, wherein the communication voice device is a mobile voice device.

11. A method of geographically comparing the user communication voice device and the closest public router to the user Computer signature.

12. The method of claim 11, wherein the communication voice device is a non-mobile telephone.

13. The method of claim 11, wherein the communication voice device is a mobile telephone.

14. The method of claim 11, wherein the communication voice device is a mobile voice device.

15. A method of comparing the geographical location of computer signature with the geographical location of the communication voice device of an internet user.

16. The method of claim 15, wherein the communication voice device is a non-mobile telephone.

17. The method of claim 15, wherein the communication voice device is a mobile telephone.

18. The method of claim 15, wherein the communication voice device is a mobile voice device.

19. A method of identifying an internet user by assigning the internet user mobile phone geographical location to the internet user gateway Mac address

20. A method of identifying an internet user by assigning the internet user mobile phone geographical location to the internet user network card Mac address

21. A method of identifying an internet user by assigning the internet user mobile phone geographical location to a unique identifier in the computer

22. A method of identifying an internet user by assigning the internet user mobile phone geographical location to a unique identifier in the internet user network device.

23. A method of identifying an internet user by assigning the internet user mobile phone geographical location a combination of identifiers of the internet user network or computer.

24. A method of identifying an internet user by a geographical comparison between the internet user mobile phone geographical location and the internet user gateway Mac address geographical location.

25. A method of identifying an internet user by a geographical comparison between the internet user mobile phone geographical location and the internet user network card Mac address.

26. A method of identifying an internet user by a geographical comparison between the internet user mobile phone geographical location and the internet user unique identifier in the computer.

27. A method of identifying an internet user by a geographical comparison between the internet user mobile phone geographical location and the internet user network device.

28. A method of identifying an internet user by a geographical comparison between the internet user mobile phone geographical location and the internet user combination of computer and network identifiers.

received by the International Bureau on
25 July 2008.

1. Λ method of authenticating interne! user identity, comprising the steps of:

   a) creating a computer signature by identifying a specific computer having one or more characteristics;

   b) associating said computer signature with a geographic location;

   c) determining a geographical location of a wireless communication device of such internet user; and

   d) comparing said geographical location associated with said Compulcr signature with said geographical location of said wireless communication device of such internet user,

2. The method of claim 1, wherein said computer signature is created from one or more characteristics selected from the following list: Computer Network Mac address, CPIi serial number, Operating System S/N, Gateway Mac Address, operating system version. Router Mac Address, disk size, inierncl browser version, hardware installed on the computer, network card speed, operating system patches, CPU speed, memory size, virtual memory size, cookie, and software installed on the computer.

3. The method of claim 1, further comprising the step of determining if a result obtained by said comparing of said geographical location of said computer signature of such internet user wilh said geographical location of said wireless communication device of such internet user is within a predetermined distance value.

4. The method of claim 1, wherein said wireless communication device comprises at least one of a:

AMENDED SHEET (ARTICLE 19)

d) Personal Digital Assistant ("PDA");

e) mobile telephone;

f) mobile voice device; and

g) device wilh wireless internet capability .

5, A method oflocaling a router's geographical location based on at least one of:

a) an internet user's wireless communication device's geographical location; and

b) a geographic location associated with an internet user's computer signature.

6, The method of claim 5, wherein said wireless communication device comprises at least one of a:

a) PDA:

b) mobile telephone;

c) mobile voice device; and

d) any device with wireless internet; capability.

7. A method of geographically comparing a geographic location associated with an internet user's computer signature with a geographic location oi'a public router closest to such internet user.

8. The method of claim 7, wherein said wireless communication device comprises at least one of a:

a) PDA;

b) mobile telephone;

c) mobile voice device; and

d) device with wireless internet capability,

9. A method of comparing a geographical location associated with an internet user's computer signature with a geographical location of a wireless communication device of such internet user.

10. The method of claim 9, wherein said wireless communication device comprises at least one of a:

   a) PDA;

   b) mobile telephone;

   c) mobile voice device; and

   d) device with wireless internet capability.

11. A method of identifying an internet user by &geographical comparison between such internet user's mobile phone geographical location and such internet user's combination of computer and network identifiers.

12. A method of authenticating the identity of an internet user by a geographical comparison between such internet user's mobile phone location and a location associated with at least one of such internet user's:

   a)   internet user gateway Mac address;

   b)   network card Mac address;

   c)   computer;

   d)   identifier in such internet user's network device;

   c)   identifier in such internet user's computer hardware;

   f)   identifier in such internet user's computer software;

   g)   cookie;

   h)   combination of identifiers comprising at least one of such internet user's network characteristics and such internet user's computer characteristics;

   i)   gateway Mac address geographical location;

   j)   identifier in such internet user's computer; and

   k)   network device characteristics,

13, A method of making a geographic comparison between a location associated with a computer signature and a geographic location associated with an Internet Protocol.

14, The method of claim 13, wherein said computer signature can be created with at least one of:

       a) an identifier in such internet user's computer hardware;

       b) an identifier in such internet user's computer software;

       c) a cookie; find

       d) an identifier in such internet user's network device.

15, The method of making a geographic comparison between a location associated with a computer signature and a geographic location of a router,

16, The method of claim {5, wherein said computer signature can be created by at least one of:

       a) an identifier in such internet user`s computer hardware;

       b) an identifier in such internet user's computer software;

       c) a cookie; and

       d) an identifier in such internet user's network device.

17, Λ method of geographic comparison between a location associated with a computer signature and a geographic location of a mobile phone.

18, The method of claim 17, wherein said computer signature can be created by at least one of a:

       a) an identifier in such internet user's computer hardware;

       b) an identifier in such internet user's computer software;

       c) a cookie; and

d) an identifier in such internet user's network device.

STATEMENT UNDER ARTICLE 19(1)

Claims 1-4 have been amended to avoid lhe references and to improve clarity.

Claims 5 and 6 have been deleted, with some of their subject matter incorporated in amended claim 4,

Claim 7 has been amended to avoid the references and to improve clarity.

Claim 8 has been deleted.

Claim 9 has been amended Io avoid the references and to improve clarity.

Claim 10 has been deleted, with its subject matter incorporated in amended claim 7.

Claims 11 and 12 have been amended to avoid the references and to improve clarity.

Claims 13- 14 have been deleted, with some of their subject matter incorporated into amended claim 12,

Claims 15 and 16 have been amended to avoid the references and to improve clarity.

Claims 17-18 have been deleted, with some of their subject matter incorporated into amended claim 16.

Claims 19 and 20 have been amended to avoid the references and Io improve clarity,

Claims 21-28 have been deleted, with some of their subject matter incorporated into amended claim 20.

New claims 29-34 (renumbered 13-18) have been added to replace some deleted claims and to more completely claim the subject matter of the specification.

Applicant respectfully submits that the amendments distinguish applicant's claims from the disclosures of the references cited in the ISR, The Pok d reference, by its own admission, does not work with mobile communication devices. Applicant believes that no new matter is introduced by these amendments. Applicant's invention uses two authentication paths. Applicant respectfully disagrees with the searcher's assessment as to inventive step. It is by an inventive step that applicant's claimed methods became possible.
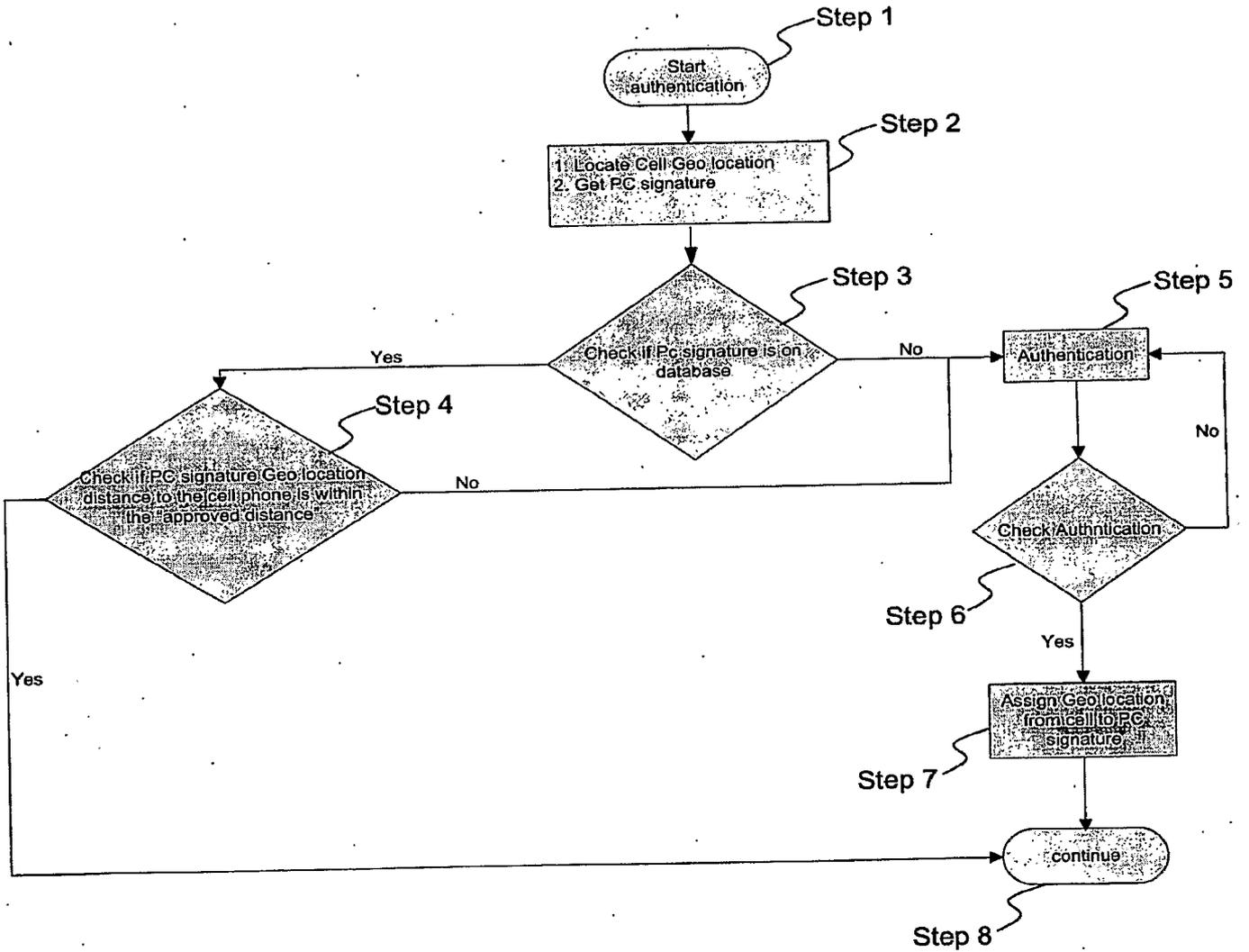
FIG. 1

INTERNATIONAL SEARCH REPORT	International application No.
	PCT/US07/12552

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **H04L** 9/00(2006.01)

USPC: 726/3

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
   U.S. : 726/3; 713/161 ; 370/3 10

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
US-PGPUB, USPAT, USOCR, FPRS, EPO, JPO, DERWENT, IBMJTDM, GOOGLE

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2002/001683 1 A1 (Peled et al.) 07 February 2002 (07.02.2007), abstract and paragraphs 14,19, 28-29, 53, 55, 63-66, 146, 186, 191, 193-194, 206-214	1-3, 7, 11, 15 19-28 ----------- 4-6, 8-10, 12-14, 16-18
Y	US 2003/0134648 A1 (Reed et al.) 17 July 2003 (17.07.2003), abstract and paragraphs 14, 152, 665, 760, 916, 1054, 1140, 1323	4-6, 8-10, 12-14, 16-18

☐ Further documents are listed in the continuation of Box C.   ☐ See patent family annex.

• Special categories of cited documents	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance		
"E" earlier application or patent published on or after the international filing date	"X"	document of particular relevance, the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"	document of particular relevance, the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O" document referring to an oral disclosure, use, exhibition or other means		
"P" document published prior to the international filing date but later than the priority date claimed	"&"	document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 May 2008 (16.05.2008)	28 MAY 2008

Name and mailing address of the ISA/US
   Mail Stop PCT, Attn ISA/US
   Commissioner for Patents
   P O Box 1450
   Alexandria, Virginia 223 13-1450
Facsimile No. (571) 273-3201
	Authorized officer
	
	HADI ARMOUCHE
	
	Telephone No. 5 17-272-2100

Form PCT/ISA/210 (second sheet) (April 2007)