

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
10 April 2008 (10.04.2008)

PCT

(10) International Publication Number
WO 2008/040539 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04M 3/436* (2006.01)

69245 Bammental (DE). **BRUNNER, Marcus** [DE/DE];
Hermann-Oberth-Weg 2, 69181 Leimen (DE).

(21) International Application Number:
PCT/EP2007/008610

(74) Agent: **ULLRICH & NAUMANN**; Luisenstrasse 14,
69115 Heidelberg (DE).

(22) International Filing Date: 4 October 2007 (04.10.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10 2006 047 275.6 4 October 2006 (04.10.2006) DE

(71) Applicant (for all designated States except US): **NEC EUROPE LTD.** [DE/DE]; Kurfürsten-Anlage 36, 69115 Heidelberg (DE).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **STIEMERLING, Martin** [DE/DE]; Karl-Gehrig-Weg 15, 69118 Leimen (DE). **DIETZ, Thomas** [DE/DE]; Frankenweg 2, 67366 Weingarten (DE). **TARTARELLI, Sandra** [IT/DE]; Hedwig-Kettler-Strasse 6, 76137 Karlsruhe (DE). **EWALD, Thilo** [DE/DE]; Im Centgrafenberg 16, 69181 Leimen (DE). **GIAKAS, Enrico** [DE/DE]; Karl-Gehrig-Weg 7, 69181 Leimen (DE). **QUITTEK, Jürgen** [DE/DE]; Daimlerweg 15, 69226 Nussloch (DE). **NICCOLINI, Saverio** [IT/DE]; Carl-Philipp-Fohr-Strasse 4, 69121 Heidelberg (DE). **STÜTTGEN, Heinrich** [DE/DE]; Im Degen 21,

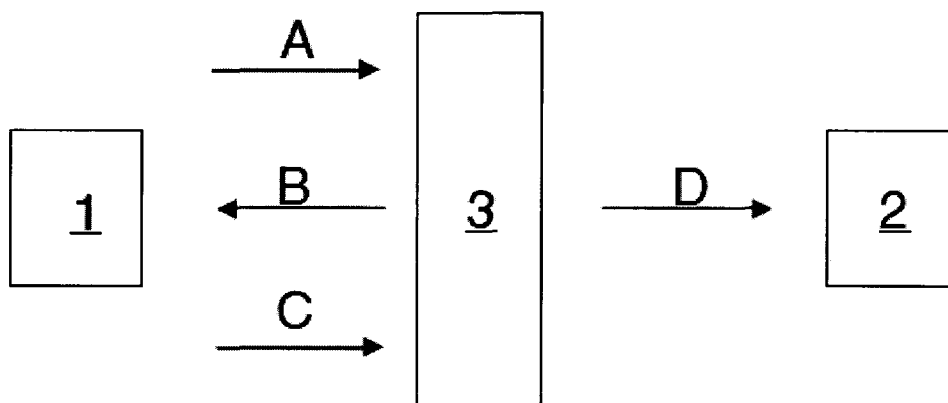
(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP,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

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

- with international search report
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

(54) Title: A METHOD FOR ESTABLISHING A CONNECTION ORIENTED COMMUNICATION AFTER SCREENING THE CALL FOR DESIRED CHARACTERISTICS



(57) Abstract: A method for establishing a connection oriented communication, preferably in the form of a telephone connection via the Internet, between a first communication partner as calling party, caller (1), and a second communication partner as called party, callee (2), wherein the caller (1) directs a request for establishing a connection to the callee (2), is characterized with respect to effectively suppressing SPAM calls with minimum interference of normal telephone operations in that on the side of the callee (2), after receiving the request for establishing a connection, initially the origin of the request is checked, and based on the result of the analysis it is decided whether to establish a connection, or to decline the request temporarily. Feature is known in the field of SPIT, SPAM over IP or more generally as an unsolicited multimedia call as Greylisting (or Graylisting).

WO 2008/040539 A1

A METHOD FOR ESTABLISHING A CONNECTION ORIENTED COMMUNICATION

The invention relates to a method for establishing a connection oriented communication, preferably in the form of a telephone connection via the Internet, between a first communication partner as calling party, caller, and a second communication partner as called party, callee, wherein the caller directs a request for establishing a connection to the callee.

In the area of electronic mail unsolicited bulk email messages – so-called SPAM – have become very common and have turned into a severe problem. Not only companies that require email communication are impacted by SPAM messages, but also private users are very annoyed by SPAM. Many Internet users nowadays receive more SPAM messages than regular emails. For this reason, almost every server for incoming email uses SPAM filters which check incoming mails according to defined rules. They search, for example, actively for key words in the content of an email, they check specific configurations of the server used for sending the email or they search for senders that are often used for sending bulk emails. In case of a matching classification of an email as SPAM, it is marked and/or sorted out.

In the area of telephone communication, analog or digital, SPAM also occurs increasingly, which occurs there, for example, as unsolicited commercial calls, and which is generally designated as SPIT (SPAM over Internet Telephony). These calls are mostly placed by automated calling machines. Due to the currently and mainly employed switched telephone networks, such SPAM calls are very cumbersome and expensive which is the reason for a rather restricted number of SPAM calls. When Internet telephony will be used more commonly though, such SPAM calls will become much easier and cheaper, so a tremendous increase of SPAM calls will have to be assumed. Therefore, also here a respective filtering of the calls according to certain rules is necessary.

Many methods, which are being used in the context of email SPAM filters, cannot be transferred to the area of telephone communications, or can only be transferred with significant modifications. The reason for this is the different nature of the two types of

communication. While email uses an asynchronous data transfer, in which the entire content can be examined, and in which a delay in the transmission is acceptable, telephone calls and similar forms of communication require the establishment of real time communication sessions. Thus, neither the content can be examined, nor delays can be tolerated.

It is therefore an object of the present invention to improve and further develop a method of the initially described type for establishing a connection oriented communication in such a way, that unsolicited SPAM calls can be effectively prevented, wherein the regular telephone operation shall be influenced as little as possible and a disturbance of telephone communication participants shall be mostly avoided.

In accordance with the invention, the aforementioned object is accomplished by a method comprising the features of claim 1. According to this claim, such a method is characterized in that on the side of the callee, after receiving the request for establishing a connection, initially the origin of the request is checked, and based on the result of the analysis it is decided whether to establish a connection, or to decline the request temporarily.

According to the invention, it has first been recognized that a method for avoiding undesired communication connections has to get involved already before the actual establishment of the connection. According to the invention, initially the arrival of a request for a connection establishment is awaited. After receiving the request for a connection establishment, the establishment of a connection is initially deferred and an analysis of the origin of the request is performed. Then, based on the result of the analysis, a decision is made whether to establish a connection, or whether to decline the request on a temporary basis. Since an origin analysis can be performed rather quickly, there are no significant delays and the communication operation between the communication participants is only influenced minimally. A request for a communication establishment from a dubious origin, which raises the suspicion that it could be a SPIT call, is declined according to the invention only on a temporary basis, whereby – in contrast to the situation where it is declined ultimately – the opportunity for further handling is given.

In an advantageous manner, it is checked in the context of the analysis whether the caller is known to the callee. Requests for communication establishment from known parties can generally be classified as non critical. Accordingly, the connection can always be established for those callers already known in advance.

With respect to an efficient and fast familiarity check, it may be provided that a list is maintained on the side of the callee, which could be designated as white list, and in which callers are listed, which are known to the callee, e.g. due to calls made in the past.

In particular for the case that the check yields that the request comes from a caller, which is not known to the callee, a temporary declining of the incoming request may be provided. In this context, the fact is being used, that a major percentage of SPIT calls is generated by so-called Bot-Networks. Typically, a Bot-Network is a large set of network computers, which have been modified by spammers in an illegal manner. Spammers use security gaps of the network computers for this purpose to install SPAM software on them. This is typically performed without being noticed by the regular operator of the computer. Generally, spammers use software, which performs an automatic penetration into the computers, thus generating Bot-networks, which can easily comprise several thousand computers. Since these computers are generally not known to the callee, a temporary declining of connection requests from unknown callers constitutes an efficient SPIT suppression.

Moreover, in the context of analyzing the origin of the request, a reverse DNS (domain name system) resolution can be attempted. Depending on requirements and individual wishes of the callee, it may then be provided that requests from unknown callers are not declined temporarily in general, but only when the DNS resolution proves to be unsuccessful.

In a particularly advantageous manner, the caller is informed about the temporary declining of its request. In this context, the caller can furthermore be informed about the reason for being declined, i.e. it can be communicated to the caller that the request has been declined for the purpose of avoiding SPAM calls.

Furthermore, in case of a temporary declining of an incoming request, a waiting period and a subsequent time window for a second call of the caller can be set. The length of the wait period as well as the length of the time window can be determined as freely configurable parameters. It may furthermore be provided, that the caller is asked to send a second request for establishing a connection within the predetermined time window. In the case that a second request of the caller is performed within the predetermined time window, it may be provided, that the connection with the callee is established. This measure takes advantage of the fact, that spammers use single computers generally only for short periods of time in order to avoid to be discovered by the regular operator of the computer. A typical spammer behavior is that spammers attempt to place as many SPAM calls as possible during the time in which they use the computers. For this reason spammers like to use so-called "fire-and-forget" approaches for SPIT production. This means that the further fate of the placed calls, in particular their connection status, is generally not followed-up any further by the spammers. Accordingly, it is very unlikely that SPIT calls generated in this manner are being repeated within the predetermined time window, so that by employing the described measure an efficient suppression of undesired communication connections is realized.

With respect to a long term usage of information once generated, it may be provided that a caller, which performs a second request within the predetermined time window, is entered into a white list. In case of future requests, this party can thus be considered as known, and the connection can be directly established without further checks.

In the context of a particularly preferred embodiment the signaling protocol for the connection oriented communication, which, e.g., can be the Session Initiation Protocol (SIP), is extended by an explicit signal. In case of a request for establishing a connection from an unknown caller, this signal is sent from the callee to the caller. Alternatively, the signal can be sent to the caller by a signaling server on the signaling path of the respective connection, or by any other suitable network entity located on the signaling path. Via the signal, the caller is informed about the temporary declining of its request.

With respect to an easy identification of a potential second calling attempt, it may be provided that the sender of the signal stores an identification of the caller. In particular, this identification can be, e.g., the address of the caller. Alternatively, or additionally, an identification of one of the signaling servers, which have passed on the request for establishing a connection, can be stored. On the side of the caller, it may be provided that it automatically sends a second request for establishing a connection within the predetermined time window, when receiving the signal.

If the caller does not send a second request for establishing a connection within the predetermined time window, it may be provided that the stored identification of the caller is deleted. In other words, the caller is again listed in some kind of gray list. This means that in case of a new request the procedure of origin checking is performed again, before determining whether a connection is established.

With respect to a particularly high level of security it may be provided that a label is assigned to the caller, which is added to the signal. The establishment of a connection upon the second request for establishing a connection can then be based on the fact of whether or not the caller uses its assigned label.

Alternatively or additionally, it is conceivable to append a challenge to the signal. The establishment of the connection upon the second request for connection establishment can then be based on the fact of whether or not the caller has resolved the challenge. The challenge can be performed e.g. as a mathematical puzzle, or as any other question, which is selected in such a way that it can be resolved by software used to generate SPIT only with a certain time effort.

With respect to an implementation that is as simple as possible and which does not require any additional signaling, it may be provided that the caller is initially asked with a recorded voice message to send another request for establishing a connection within the predetermined time window. The recorded voice message can furthermore comprise the information that the refusal constitutes a measure for avoiding SPAM calls. The voice message can be recorded in several different languages. If the request for establishing a connection comprises information with respect to the language preferred by the caller, which can e.g. be supported by the Session

Initiation Protocol (SIP), the recorded message can be played in the respective language, in order to assure that the caller understands the message.

With respect to a further improvement of security, the callee can distribute number codes to potential calling parties as a precaution. In case of a request for establishing a connection, it can be checked if the caller has a valid number code. If this is the case, a connection is established, otherwise the call is declined. Alternatively, a white list can be generated by the callee as a precaution, in which those callers are listed, whose calls are not to be identified as SIP.

In the context of another preferred embodiment, it is provided, that an unknown caller is requested to leave a message on a voice mail box of the callee. Thus, a rerouting of a call can be performed onto the voice mail box for each call of an unknown caller. It is also conceivable that a rerouting is only performed, when the caller has previously selected this option, e.g. through using dial tones.

A telecommunications service provider can provide the described functions in an advantageous manner to its customers as an added value service, or as a service to be billed separately, or together with other services.

There are several ways how to design and further develop the teaching of the present invention in an advantageous way. To this end, it is to be referred to the patent claims subordinate to patent claim 1 on the one hand and to the following explanation of preferred embodiments of the invention by way of example, illustrated by the figure on the other hand. In connection with the explanation of the preferred embodiment of the invention by the aid of the figure, generally preferred embodiments and further developments of the teaching will be explained. In the drawing,

Fig. 1 shows an embodiment of a method according to the invention for establishing an internet telephone communication between two communication partners, and

Fig. 2 shows an embodiment of a time structure for an identification of SPIT calls.

Fig. 1 schematically shows an embodiment of a method according to the invention for establishing an internet telephone connection between a caller 1 and a callee 2. In the illustrated embodiment, the entire functionality for avoiding the connection of SPIT calls is implemented in a signaling server 3, which is located in the signaling path between the communication partners 1, 2, and in front of the terminal of the callee 2. It is appreciated that the functionality for avoiding SPIT can also be implemented directly in the terminal of the callee 2 in another embodiment.

As it is apparent in Fig. 1, the caller 1 initially sends a request A for establishing a connection to the callee 2. This can be performed e.g. based on the Session Initiation Protocol (SIP). The SPIT defense system 3 checks the origin of the request, or by comparing the address of the caller 1 with the stored addresses of callers, known to the callee 2. Thus, callers can e.g. be defined as known, when they have already previously successfully placed a call with the callee 2. The callee 2, however, can define permitted callers also in the form of a white list.

In case the check yields, that the caller 1 is a known, and thus a permitted party, a connection is immediately established. This means the call is connected to the callee 2. In Fig. 1, the case is shown, where the caller 1 is a caller, who has not been known so far. For handling such calls, the employed signaling protocol is expanded by a signal, which is transmitted by the SPIT defense system 3 (or alternatively by the terminal of the callee 2) to the terminal of the caller 1. The signal, designated with B in Fig. 1, communicates to the caller 1, that the call has been declined in a preliminary manner, and asks the caller to call again at a later point in time. The request can furthermore comprise the specification of a time window and read accordingly: "Please call again within the next five minutes (within the next hour)".

The sender of the signal B stores an identifier of the caller 1, or its terminal, or an identifier of one of the signaling servers, which have routed the request for establishing a connection. Storing an identifier serves for later identification of a

second calling attempt. The second call, if it is performed within the specified time window, will pass the SPIT defense system and will cause that the terminal of the callee sends a ring tone. The second call is designated in Fig. 1 with the designation C. The successful establishment of a connection with the callee 2 is designated with a designation D.

However, if the second call is not placed within the specified time window, the stored identifier of the caller 1 is deleted again. A new calling attempt is correspondingly treated like a first calling attempt, and again has to go through a check by the SPIT defense system as described above.

The described approach requires a standardization of the signal B, which is sent from the callee 2 to the caller 1, and an expansion of the user interface of the terminal of the caller 1 in order to show the received signal to the caller and possibly to provide a mechanism for automatic generation of a second calling attempt. According to an alternative approach, this is less convenient for the caller 1, but does not require a standardization of signals. The SPIT defense system is provided so that a call from an unknown caller is established, however, only for the purpose to transmit a recorded language message from the callee 2, asking the caller 1 to call again within a predetermined time window.

Fig. 2 shows a time axis in a schematic illustration, showing the time based operation of a SPIT defense system in an exemplary manner. At the point in time, designated t_0 , a first call attempt of a caller 1 comes in at the callee 2. Since the caller 1 is not known to the callee 2, the call is initially declined as described above in detail, and a waiting time and a subsequent time window for a second call attempt of the caller 1 is determined. In a practical application, a point time, t_1 , and a point in time, t_2 , are determined. A new calling attempt of a caller within the time interval between the points in time t_0 and t_1 is finally declined. Calls within the time window, defined by the points in time, t_1 and t_2 , however, are accepted. The address of a party 1 calling again between the points in time t_1 and t_2 can, on the one hand, be stored on the side of the callee 2 in a white list, and future calls of this party can be connected with the callee 2 without further checking.

After the time window has expired, this means after the point in time t_2 , the stored address of the caller 1 is deleted. A second call occurring after the point in time t_2 of the caller 1 is thus treated like a first call, and has to go through the SPIT check again.

Many modifications and other embodiments of the invention set forth herein will come to mind the one skilled in the art to which the invention pertains having the benefit of the teachings presented in the foregoing description and the associated drawings. Therefore, it is to be understood that the invention is not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

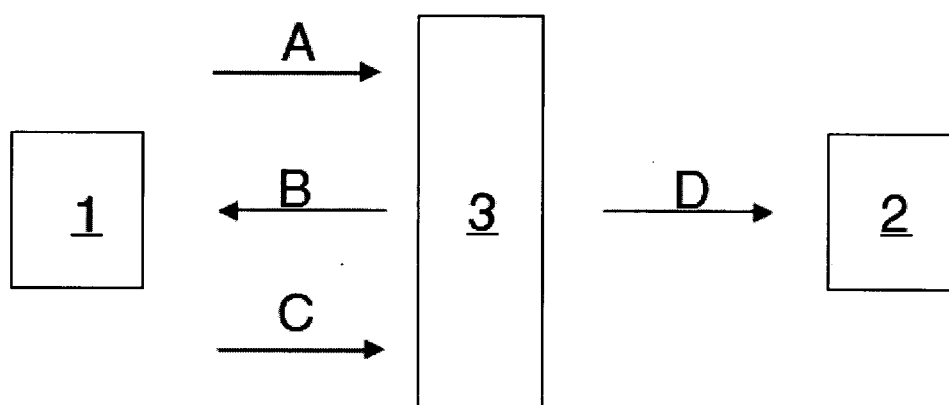
Claims

1. Method for establishing a connection oriented communication, preferably in the form of a telephone connection via the Internet, between a first communication partner as calling party, caller (1), and a second communication partner as called party, callee (2), wherein the caller (1) directs a request for establishing a connection to the callee (2),
c h a r a c t e r i z e d i n that on the side of the callee (2), after receiving the request for establishing a connection, initially the origin of the request is checked, and based on the result of the analysis it is decided whether to establish a connection, or to decline the request temporarily.
2. Method according to claim 1, wherein it is checked in the context of the analysis, whether the caller (1) is known to the callee (2).
3. Method according to claim 2, wherein a list is maintained on the part of the callee (2), in which callers are listed, which are known to the callee (2).
4. Method according to claim 2 or 3, wherein a request received by the callee (2) is temporarily declined, if the request comes from a caller (1), which is not known to the callee (2).
5. Method according to any of claims 1 to 4, wherein a request received by the callee (2) is temporarily declined, if a reverse DNS (domain name system) resolution of the address of the caller (1) is not successful.
6. Method according to any of claims 1 to 5, wherein the caller (1) is informed about the temporary declining of its request.
7. Method according to any of claims 1 to 6, wherein in case of a temporary declining of an incoming request, a waiting period and a subsequent time window of predeterminable lengths are determined for a second call of the caller (1).

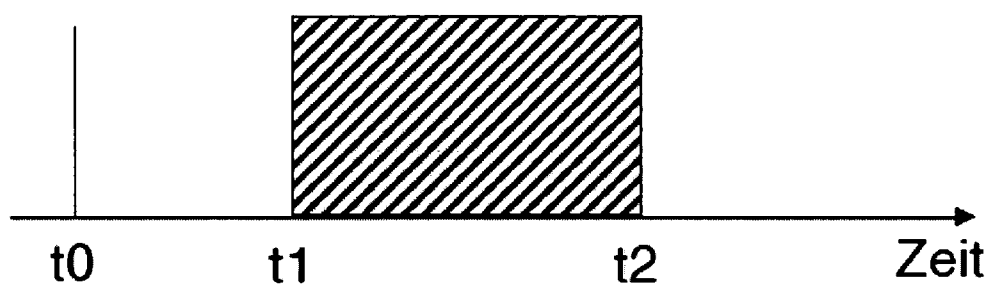
8. Method according to claim 7, wherein the caller (1) is requested to send a second request for establishing a connection within the predetermined time window.
9. Method according to claim 7 or 8, wherein in case of a second request of the caller (1) within the predetermined time window, the connection with the callee (2) is established.
10. Method according to any of claims 7 to 9, wherein the caller (1) is entered into a white list, in case of a second request within the predetermined time window.
11. Method according to any of claims 2 to 10, wherein in the context of the signaling protocol for the connection oriented communication, a signal is provided, which in case of a request for establishing a connection from the side of an unknown caller (1), is sent to the caller (1), either by the callee (2), or by a signaling server in the signaling path of the respective connection.
12. Method according to claim 11, wherein the sender of the signal stores an identification of the caller (1), or an identification of one of the signaling servers, which have forwarded the request for establishing a connection.
13. Method according to claim 11 or 12, wherein on the side of the caller (1), when receiving the signal, a second request for establishing a connection is automatically sent within the predetermined time window.
14. Method according to claim 12 or 13, wherein the stored identification of the caller (1) is deleted in case no second request for establishing a connection is transmitted by the caller (1) within the predetermined time window.
15. Method according to any of claims 11 to 14, wherein a label assigned to the caller (1) is added to the signal, wherein the connection, upon the second request for establishing a connection, is established only in case the caller (1) uses the assigned label.

16. Method according to any of claims 11 to 15, wherein a challenge is added to the signal, wherein the connection, upon the second request for establishing a connection, is established only in case the caller (1) has resolved the challenge.
17. Method according to any of claims 1 to 16, wherein the caller (1) is requested by means of a recorded voice message to send a new request for establishing a connection within the predetermined time window.
18. Method according to claim 17, wherein the recorded voice message is provided in several different languages.
19. Method according to claim 18, wherein on the part of the caller (1) a preferred language is designated in the context of the request for establishing a connection, and wherein the recorded voice message is played in the preferred language.
20. Method according to any of claims 1 to 19, wherein on the part of the callee (2) number codes are distributed to potential calling parties in advance, and wherein in case of a request for establishing a connection, a connection is established, if the analysis of the origin of the request yields that the caller (1) has a valid number code.
21. Method according to any of claims 1 to 20, wherein on the part of the callee (2) a white list is established in advance, and wherein in case of a request for establishing a connection, a connection is established, if the analysis of the origin of the request yields that the caller (1) is listed in the white list.
22. Method according to any of claims 1 to 21, wherein an unknown caller (1) is requested to leave a message on the voice mail box of the callee (2).
23. Method according to any of claims 1 to 22, wherein the functions are provided by a telecommunications service provider to customers as a value added service, or as an additional chargeable service separately or bundled with other services.

1/2

**Fig. 1**

2/2

**Fig. 2**

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2007/008610

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04M3/436

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L H04M

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

Electronic data base consulted during the International search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	ROHWER T ET AL: "TNG White Paper: Abwehr von Spam over Internet Telephony (SPIT-AL)" INTERNET CITATION, [Online] 31 January 2006 (2006-01-31), XP007902521 Retrieved from the Internet: URL: http://www.spit-abwehr.de/Whitepaper_SPITAL_20060310.pdf [retrieved on 2007-06-15] page 10, paragraph 3 - page 18, paragraph 6 ----- -/--	1-23

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- * & * document member of the same patent family

Date of the actual completion of the international search

18 January 2008

Date of mailing of the international search report

29/01/2008

Name and mailing address of the ISA/
European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Nash, Michael

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2007/008610

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EVAN HARRIS: "The Next Step in the Spam Control War: Greylisting" INTERNET CITATION, [Online] 21 August 2003 (2003-08-21), XP002446302 Retrieved from the Internet: URL: http://projects.puremagic.com/greylisting/whitepaper.html> [retrieved on 2007-08-09] the whole document -----	1-23