BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS

BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE

CHAMBRES DE RECOURS DE L'OFFICE EUROPEEN DES BREVETS

Internal distribution code:
(A) [ ] Publication in OJ
(B) [ ] To Chairmen and Members
(C) [ ] To Chairmen
(D) [X] No distribution

Datasheet for the decision of 3 July 2013

Case Number: T 2309/08 - 3.5.06

Application Number: 04018959.9

Publication Number: 1513042

IPC: G06F 1/00

Language of the proceedings: EN

Title of invention:
Coordinated network initiator management that avoids security conflicts

Applicant:
MICROSOFT CORPORATION

Headword:
Initiator management/MICROSOFT

Relevant legal provisions (EPC 1973):
EPC Art. 83
EPC R. 27 (1) (e)

Keyword:
"Insufficient disclosure - all requests"

Decisions cited:
-

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 2309/08 - 3.5.06

D E C I S I O N
of the Technical Board of Appeal 3.5.06
of 3 July 2013

Appellant: (Applicant)
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052 (US)

Representative:
Grünecker, Kinkeldey
Stockmair & Schwanhäusser
Leopoldstrasse 4
D-80802 München (DE)

Decision under appeal:
Decision of the Examining Division of the European Patent Office posted 8 July 2008 refusing European patent application No. 04018959.9 pursuant to Article 97(2) EPC.

Composition of the Board:

Chairman: D. H. Rees
Members: M. Müller
W. Sekretaruk

Summary of Facts and Submissions

I. The appeal lies against the decision of the examining division, dated 8 July 2008, to refuse European patent application 04018959.9 for lack of an inventive step.

II. Notice of appeal was filed on 17 September 2008, the appeal fee being paid on the same day. With a statement of grounds of appeal, received on 13 November 2008, the appellant filed claims according to a main request and auxiliary requests I to VI and requested that the decision under appeal be set aside and a patent be granted based on one of these seven sets of claims.

III. With summons to oral proceedings the board informed the appellant of its preliminary opinion, raising objections under Article 83, 84 and 56 EPC 1973.

IV. In response, the appellant filed eight amended sets of claims according to a main request and auxiliary requests I to VII. During oral proceedings the appellant filed further auxiliary requests VIII and IX.

V. The appellant requested that the decision be set aside and that a patent be granted based on claims 1-19 according to the main request or auxiliary requests I and III, claims 1-18 according to auxiliary requests II, IV or VI, claims 1-15 according to auxiliary request V or claims 1-14 according to auxiliary requests VII to IX, in combination with drawings 1-3 and description pages 1, 2, and 4-13 as originally filed and description page 3 as filed on 29 January 2007.

VI. Claim 1 according to the *main request* reads as follows.

"A method in a computer system (201), wherein the computer system is a computer or a hand-held device, that includes a plurality of initiators (230), each for initiating communication with target devices (250) over a network (240), in particular, each initiator being an iSCSI initiator, the method for configuring the computer system (201) to securely communicate with a target device (251-255) over the network (240), the method comprising the following performed by an abstraction module (220) that configures each of the plurality of initiators (230) in a manner that security conflicts between the plurality of initiators (230) is avoided:

an act of exposing a common interface for configuring any of the plurality of initiators (230);

an act of receiving an indication through the common interface that a selected initiator from among the plurality of initiators (230) is to be configured to communicate with a selected target device;

an act of retrieving security information from a database (261) that includes information that is relevant to configuring security for any of the plurality of initiators (230);

an act of identifying a security configuration of the selected initiator using the retrieved security information, the identified security configuration including the retrieved security information which may have been further processed by the abstraction module;

an act of determining that the identified security configuration would not cause the selected initiator to conflict with any of the other of the plurality of initiators (230); and

an act of configuring the selected initiator using the identified security configuration."

Claim 1 of *auxiliary request I* is identical to that of the main request, except that the "act of exposing a common interface" has been limited by the following statement:

"... wherein the common interface is an Application Programm Interface API".

Claim 1 of *auxiliary request II* is identical to that of the main request, except that the second clause relating to the "act of identifying a security configuration" has been amended to read as follows:

"... the identified security configuration including the retrieved security information *being* further processed by the abstraction module" (emphasis by the board).

Claim 1 of *auxiliary request III* is identical to that of the main request, except that between the "act of determining" and the "act of configuring" the following phrase has been inserted:

"... if a conflict is determined, an act of reconfiguring other initiators so that a conflict is

eliminated and/or identifying another security configuration; ...".

Claim 1 of *auxiliary request IV* is identical to that of the main request, except that at the end the following phrase has been inserted:

"... wherein the indication through the common interfaces is received in response to a request to communicate with the selected target device".

Claim 1 of *auxiliary request V* is identical to that of the main request, except that at the end the following phrase has been inserted:

"... wherein the retrieved security information comprises IPSec configuration information or CHAP configuration information".

Claim 1 of *auxiliary request VI* is identical to that of the main request, except that "in particular" has been deleted and each occurrence of the term "initiator" or "initiators" has been amended to read "iSCSI initiator" or "iSCSI initiators", respectively.

Claim 1 of *auxiliary request VII* is identical to that of auxiliary request VI, except that at the end the following phrase has been inserted:

"... wherein the retrieved security information comprises IPSec configuration information".

Claim 1 of *auxiliary request VIII* is identical to that of auxiliary request VII, except that in the "act of

identifying" the clause "which may have been further processed by the abstraction module" has been deleted and at the end the following phrase has been added:

"... wherein the identified security configuration is the same as the retrieved security information".

Claim 1 of *auxiliary request IX* is identical to that of auxiliary request VIII, except that between the "act of determining" and the "act of configuring" the following has been added:

"... an act of, if a conflict does exist, identifying another security configuration for the selected initiator; ...".

For completeness it is noted that each request contains another independent computer program product claim which corresponds closely with the respective method claim.

VII. At the end of the oral proceedings, the chairman announced the decision of the board.

Reasons for the Decision

The invention

1. The application generally relates to the communication between a computer and possibly remote peripheral devices over the Internet. More specifically, the application relates to iSCSI: SCSI is short for Small Computer System Interface, and iSCSI, short for Internet

SCSI, is a protocol for carrying SCSI commands over networks using the TCP/IP protocols of the Internet. The computer contains a so-called "initiator" which functions as an iSCSI client. The peripheral devices on remote servers are referred to as "targets".

1.1 IP-based communication over the Internet in general, and iSCSI communication in particular, is vulnerable to interception, eavesdropping or hijacking so that additional security provisions may be required. The description discloses that established IP security standards may be used to this end such as IPSec or CHAP (CHallenge Authentication Protocol; see original description, p. 2, lines 12-17; p. 12, lines 8-10; and original claims 4 and 5).

1.2 The description mentions that "IPSec supports a variety of encryption algorithms, includes options regarding which part of the message is to be encrypted, and what type of authentication is to be employed" (p. 2, lines 18-23). It is further disclosed that "[t]he configuration settings of IPSec include whether or not to use a key, whether or not tunneling mode is desired, which encryption is to be used, and other IPSec setting options" (p. 12, line 30 - p. 13, line 1). The application does not discuss any details of CHAP or other security standards.

1.3 The description discloses that an "initiator ... must be properly configured ... in order for the communication to be secured as desired and interpretable by the target device" (p. 2, lines 21-23). In computing systems with multiple initiators, it is further disclosed that "initiators are typically configured without re-

garding for the security configuration of the other initiators in the computing system" and that "accordingly, sometimes conflicts arise between the security configurations of the initiators" which "may prevent [them] from functioning as intended, or even functioning at all" (p. 2, lines 23-29).

1.4 The invention therefore sets out to enable "multiple initiators on a computer system [to] be properly configured with security information in a manner that the security information of one initiator does not conflict with the security information of any other initiator" (p. 2, line 30 - p. 3, line 2).

Configuration conflicts

2. The description does not disclose details of the possible conflicts between the configurations of different initiator or how the invention is to "determin[e] that [a given] security configuration would not cause [one] initiator to conflict with any of the other of the plurality of initiators".

2.1 While the description suggests (*loc. cit.*) that the conflicts in question are caused by the presence of multiple initiators on one computer system, the board notes that it is not claimed in any of the requests nor elaborated on in the description that the conflicts concerned are such as are caused specifically by this circumstance. In particular, neither the description nor the claims exclude, in the board's view, the possibility that the relevant conflicts would (or might) also arise between multiple initiators on different computers, for instance if two initiators were to use

configurations which were incompatible with respect to a single target device. At any rate, the reference to multiple initiators is, in the board's view, insufficient to delimit substantially the range of possible conflicts.

2.2 The description discloses that conflicts may be such that the "the ability of other initiators to communicate" is "degraded" (see p. 4, line 1-3 and p. 5, lines 12-14). The above-mentioned formulation (point 1.3) that conflicts may "prevent the initiators from functioning as intended, or even functioning at all" is less specific.

3. During the oral proceedings, the appellant explained by way of two examples the kind of conflicts the application means to refer to.

3.1 An IPSec configuration determines, *inter alia*, whether "tunneling mode" or "transport mode" is to be used. Network cards may be limited to processing data packets according to only one of these modes at a time. Hence, in a computer system with multiple initiators all using the same network card having such a restriction there will be a conflict between one initiator configured to use tunneling mode and another initiator configured to use transport mode.

3.2 Another IPSec parameter determines the key length used during encryption, say 64 or 128 bit. Some encryption engines employed may require that a single key length be selected and may be incapable of encrypting different packets with keys of different lengths. Again, in a computer system where multiple initiators have to

access the same such encryption engine a conflict may arise if two initiators are configured to use different key lengths.

3.3 In these examples, the conflict arises only because multiple initiators have to use a shared component, thereby illustrating how conflicts may be caused by the presence of multiple initiators on a single computer system.

4. The board notes that neither of these examples is disclosed nor is the specific conflict mentioned or alluded to in the description. Only the "tunneling mode" is mentioned as one of several known IPSec setting (p. 12, last par.). The board also notes that both examples relate to IPSec. The appellant did not produce any example without this limitation even when invited to do so during oral proceedings.

Main request

5. Claim 1 of the main request specifies acts of "retrieving security information from a database" and "identifying a security configuration for [a] selected initiator using the retrieved information" and, centrally, an "act of determining that the identified security information would not cause the selected initiator to conflict with any of the other of the plurality of initiators".

5.1 As explained above, the description fails to define or illustrate by way of example or otherwise the conflicts that are to be avoided or how they are to be determined. Apart from indicating that conflicts might "degrade

communication", the nature of the conflicts in question is not further explained.

5.2 Security configurations as claimed may involve a large number of various parameter settings. Without any specification as to what security standard, if any, these configurations relate to the, the number of parameters is undefined. Each configuration represents a combination of several parameter settings. The appellant's examples relate to situations in which different settings of a single parameter in different configurations conflict with each other. A priori, however, conflicts might arise between the setting of a parameter A in one configuration and the setting of a different parameter B in another one, or only between the combined parameter settings in two configurations.

5.3 Whether or not a conflict would arise may depend, as the appellant's arguments illustrate, on the presence of certain, unspecified hardware or software components on the sender's side - or, as the board considers, the receiver's side - and what limitations these may put on the choice of configuration settings or the number of alternative settings they can handle at any one time.

5.4 It is also noted that errors in distributed communication contexts such as the claimed one may be very difficult to detect because they may relate to the relative timing of various events in the components involved. Thus the communication between two devices may degrade, for instance, not only because packets from one to the other do not arrive or cannot be processed, but also because they arrive too late, and in a

distributed system any of these might happen in a manner difficult or impossible to predict.

6. The board notes that the description does not contain a single example as to how the skilled person is supposed to carry out the "act of determining that [an] identified security configuration would not cause [one] ... initiator to conflict with any of the other ... initiators" and that, accordingly, the description does not even, as required by Rule 27 (1) (e) EPC 1973, describe in detail at least one way of carrying out the invention.

6.1 The appellant argued that Article 83 EPC 1973 was complied with nonetheless because, as the examples above showed (point 3), the description enabled the skilled person to put into practice at least some instances of a single embodiment of the claimed subject matter.

6.2 The board disagrees with the position that a single example or a small number of enabled embodiments will, in general, be sufficient to establish that the invention is disclosed in a manner sufficiently clear and complete for it to be carried out by a person skilled in the art. Rather, according to established jurisprudence of the boards of appeal an invention must be enabled over its full breadth to comply with Article 83 EPC 1973. Therefore, depending on the breadth and the nature of the claimed invention a small number of enabled embodiments may or may not be sufficient.

6.3 In the present case the board considers that, due to the enormous number of undefined parameters that might characterise the relevant "conflicts" to be avoided

according to the claimed invention, carrying out the invention on the basis of the description and the common knowledge alone would constitute an undue burden for the skilled person.

6.4 The board thus concludes that claim 1 of the main request, especially the act of determining whether two configurations would or would not cause a conflict, is not disclosed sufficiently clearly and completely for it to be carried out by the person skilled in the art, and so does not comply with Article 83 EPC 1973.

Auxiliary requests I-IV, VI, VII

7. The above analysis is unaffected by the difference between claim 1 of the main request and claim 1 of any of auxiliary requests I-IV and VI and therefore applies directly to these requests, too. It also applies to the auxiliary request VII: The limitation of the claimed matter to iSCSI does not, in the board's view, limit the possible nature and causes of conflicts in a significant way (see esp. points 5.2-5.4).

Auxiliary requests V, VIII, and IX

8. Claim 1 of each of these requests is limited to configuration settings according to IPSec (or CHAP).

8.1 Specifically with regard to IPSec, the appellant argued in oral proceedings that the possible parameter settings of IPSec were well-known in the art. The skilled person could thus compile a list of possible configuration settings, which will be smaller than the list of all theoretically possible parameter settings

since certain settings will be excluded in combination. The skilled person could also produce a list of pairings of possible configurations and check for each entry on this list whether a conflict arises. The results so obtained could be held in a lookup list of possible conflicts for the "act of determining" to use. Both the compilation of the lists and the checking could be performed automatically, possibly aided by an automatic simulation of the claimed communication setup. While the lists may be very large and therefore the process might take a while, compiling the lists was straightforward for the skilled person and waiting for the result did not constitute an undue burden.

8.2 The board agrees that for a given security standard, even taking into account its possibly different versions, the possible configuration settings would generally be known to the person skilled in the art. IPSec is however known for its complexity and relatively large number of parameters and possible parameter combinations.

8.3 The board's argument relating the number of possible parameter combinations to be checked (point 5.2) thus continues to hold, if to a lesser degree.

8.4 Moreover, the other arguments relating to the other relevant parameters are unaffected. Even when limited to IPSec, the possibility of a conflict will depend on a number of unspecified parameters including the dynamic behaviour of the claimed communication system (see points 5.3 and 5.4). The board therefore cannot follow the appellant's argument that the checking of possible conflicts between pairs of configuration settings can

be performed (semi-)automatically as a matter of course, *i. e.* without any explicit guidance on how to do so. In this context it is noted that the simulation of a distributed parallel system is no trivial matter.

8.5 The board therefore concludes that putting to practice the "act of determining" possible conflicts would constitute an undue burden for the skilled person based on the description alone and even if limited to the context of IPSec and that, therefore, also claim 1 of auxiliary requests V, VIII and IX do not conform with Article 83 EPC 1973.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

B. Atienza Vivancos D. H. Rees