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 24 September 2008

Case Number: T 1592/05 - 3.5.01

Application Number: 03290090.4

Publication Number: 1327934

IPC: G06F 9/455, H04L 12/24

Language of the proceedings: EN

Title of invention:
Compartmented multi operator network management

Applicant:
Alcatel Canada Inc.

Opponent:
-

Headword:
Network management/ALCATEL

Relevant legal provisions:
-

Relevant legal provisions (EPC 1973):
EPC Art. 56

Keyword:
"Inventive step (no)"

Decisions cited:
-

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 1592/05 - 3.5.01

D E C I S I O N
of the Technical Board of Appeal 3.5.01
of 24 September 2008

Appellant: Alcatel Canada Inc.
600 March Road
Kanata,
Ontario K2K 2E6 (CA)

Representative: Feray, Valérie
Feray Lenne Consult
39/41, avenue Aristide Briand
92163 Antony (FR)

Decision under appeal: **Decision of the Examining Division of the European Patent Office posted 29 July 2005 refusing European application No. 03290090.4 pursuant to Article 97(1) EPC 1973.**

Composition of the Board:

Chairman: S. Steinbrener
Members: S. Wibergh
G. Weiss

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division to refuse European patent application No. 03290090.4.

II. The following documents will be referred to:

D1: J. Dike, "A user-mode port of the Linux kernel", Proceedings of the 4th Annual Linux Showcase & Conference, 10-14 October 2000, Atlanta, USA (retrieved from the Internet);

D2: J. Dike, "User-mode Linux", Proceedings of the 5th Annual Linux Showcase & Conference, 5-10 November 2001, Oakland, USA (retrieved from the Internet).

III. According to the decision appealed, Dl was the closest prior art document. It disclosed a Linux host running a plurality of virtual machines using simulated hardware and capable of running arbitrary applications that were isolated from each other. Although D1 used a different terminology than the present application the technical features were the same. For the person skilled in the art it was well known that Linux was a Unix-type multi-user, multi-tasking network operating system with security enforcement such as access control. Dl disclosed multiple independent (isolated) Linux environments (virtual machines) for different users on top of a common Linux-based host system. Consequently, all file access, networking services and access control features well known in Unix systems were also applicable to the Linux system of Dl. The technical

problem solved by D1 was also how to provide security in a shared system on the basis of self-contained environments. The subject-matter of claim 1 therefore did not involve an inventive step.

IV. With the statement setting out the grounds of appeal, dated 25 November 2005, the appellant requested that the decision be set aside and a patent be granted based on claims 1-9 filed with the same letter.

Claim 1 read (omitting the reference signs):

1. A network management system for a communications system, said network management system including a network element under the control of operations system software and sharable by a plurality of independent operators, each operator being subject to access control, characterized in that
the network management system has a compartmented operating system with a number of compartments corresponding to the number of operators, each compartment executing the same operations system software as a separate process in isolation from other compartments, each compartment being subject to access control, and each compartment being assigned to a specific operator.

V. The appellant argued that there was a fundamental difference between the operations system software, which was the applications software controlling the network element as part of the network management system, and the operating system, which was the underlying software on which the operations systems software ran.

Claim 1 was clearly novel. By no stretch of the imagination could either Dl or D2 be described as a network management system as the term was commonly understood in the art. The fleeting reference in D1, at paragraph 4.2, to the possibility of one of the virtual machines being used as a name server did not transform the described operating system software into a network management system. Moreover, claim 1 called for each compartment to run the same operations system software. In the prior art, separate instantiations of the operating system software ran on a common shared operating system, and there was a risk of information exchange through the shared common operating system. The risk increased exponentially with the number of operators. This problem was solved by employing a compartmented operating system, such as Trusted Solaris, wherein the operations software ran as a separate process in the compartments that were completely isolated from each other. This solution was not disclosed in the prior art.

The closest prior art was not D1 but the acknowledged prior art network management system illustrated in Fig. 1 of the application. The preamble of claim 1 had been amended with this position in mind. The objective technical problem was the one set forth in the application, namely how to improve the security weakness resulting from the shared operating system required to run the operations software. The solution involved employing a compartmented operating system in which the operations software ran independently as separate and isolated processes. This was not disclosed in the prior art.

Dl was not specifically concerned with privacy issues between users. The skilled person faced with the objective technical problem defined above would have no reason to pay any special attention to this document. Dl taught how a Linux kernel could be used to create a virtual machine using simulated hardware. Its paragraph 4.2 taught that "a number of applications involve isolating users of virtual machines from each other and from the host". Several reasons were given to want isolation. One was to protect the valuable resources in the event that a hostile process destroyed data, for example, by trashing the file system. Another reason was to protect the host (of the virtual machines) from a person breaking into a particular service, such as a name server. Various other unrelated reasons were also discussed, but significantly there was no teaching in Dl of the use of the virtual machines as a means of offering privacy between users, particularly users running the same software. The underlying theme of Dl was that the virtual machines ran entirely different applications. In the case of users running the same applications, there was no teaching in Dl that there would be any reason to depart from traditional access control methods discussed in the prior art described in the patent application. Dl mentioned that the fact that the virtual machines ran on the same host opened up opportunities for "sharing and communication between them". This suggested that Dl did not disclose a truly compartmented operating system as required by the invention. One of the objectives of the invention was to ensure complete isolation of the operations software running in the different compartments. Whatever Dl disclosed, the discussion of the communications between

the virtual machines would not commend itself to a person skilled in the art seeking to address the privacy problem.

Given the true starting point of the invention, namely a network management system employing an operating system offering access control, there was no reason to suppose that a person skilled in the art would recognise the security weakness identified in the application due to the common operating system. Moreover, even if he had done so, the solution to this problem was not suggested by the Linux kernel of D1, which merely described the establishment of virtual machines for purposes that were different from the object of the invention.

D2 added little to D1. The brief discussion of "security considerations" in paragraph 3.4.1 pointed in the opposite direction of the present invention since it indicated that the users of the virtual machines "will commonly have a root access". The compartmented operating system of the present invention offered a system wherein the processes were completely isolated so that privacy concerns did not arise. On the contrary, there was in D2 a discussion about shared subsystems that "open opportunities for sharing and communication between them". This passage pointed away from the use of such a system as a solution to privacy concerns.

The cited prior art therefore did not suggest a solution to the objective technical problem.

VI. In a communication annexed to a summons to oral proceedings, the Board first observed that the novelty

of the subject-matter of claim 1 might hinge on the word "same /operations system software/", the meaning being that "the same software code is running but is operating as two separate processes", as indicated in the application, paragraph [0017].

VII. Furthermore, the Board made the following comments on the appellant's arguments in the grounds of appeal:

- it was not clear why neither D1 nor D2 could be described as a network management system if a network system or device was used;

- in the appellant's view D1 and D2 could not disclose a truly compartmented operating system because of the indication that user-mode Linux could be made to share resources. The alleged difference between a compartmented operating system and a "truly" compartmented system was vague. If D1 and D2 disclosed compartments, they also disclosed compartments that could be well isolated from each other and from the host (see D1, part 4.2), but needed not be (see D2, part 3.4). It appeared that the skilled person had a choice in this respect. D2 suggested that one reason for less isolation was to be able to share network devices (D2, p.9, left-hand column, penultimate paragraph). Maintaining appropriate isolation between users while permitting control of shared network elements thus seemed to be an aim which the present invention had in common with D1 and D2;

- as to the argument that the underlying theme of D1 was that the virtual machines ran entirely different applications, the Board failed to recognize such a

theme. D1 stated that essentially all applications that ran on the native kernel would run in a virtual machine in the same way (p.6, top). The users had the choice of application, and using the same software for similar tasks seemed even to be the most obvious one;

- the appellant had argued that the compartmented operating system of the present invention offered a system wherein the processes were completely isolated. But the invention comprised a single operating system, and whether operators were "completely" isolated or not might be a matter of opinion. Furthermore, even if Trusted Solaris was superior to user-mode Linux in this respect, this operating system per se was not the invention. It was only used in the invention.

VIII. The Board was moreover of the opinion that it could be argued that since the properties of compartmented operating systems were well known, it was obvious to use such a system whenever there was a need to isolate users. The recognition of an isolation problem would hardly be inventive in itself.

IX. By letter dated 20 May 2008 the appellant informed the Board that it would not be represented at the oral proceedings.

X. Oral proceedings, which the appellant did not attend, were held on 24 September 2008. It was verified that the appellant requested that the decision under appeal be set aside and a patent be granted on the basis of claims 1-9 submitted with the statement setting out the grounds of appeal dated 25 November 2005.

At the end of the oral proceedings the Board announced its decision.

Reasons for the Decision

1. *The invention*

As explained in the application (paragraphs [0001], [0002], [0008], [0010], [0016]), the present invention relates to communication nodes and network management systems shared by independent operators. Typically, network elements and network management systems are shared by several independent operators in carrying out independent operations. These independent operators are competitors and as such do not want other operators to have access to their network management system. In such cases the operations systems have to be tightly controlled so that security, in terms of information flow control, is maintained. The aim of the invention is to provide a network management system sharable by a plurality of operators providing a strong separation between multiple operators. This is achieved by enforcing mandatory access control within separate operating system compartments. Each compartment functions autonomously, each executing the operations system software separately and in isolation from the other compartments. The number of compartments within the operating system corresponds to the number of operators. Each compartment is accessible only by the operator to which it has been allocated and it is not reachable by other operators. "Trusted Solaris" (by Sun Microsystems) is an example of an operating system that can be used in the present invention.

2. *Technical character*

The examining division did not raise an objection under Article 52(2) EPC against claim 1. The Board notes that the claim is formulated in so general terms that it might include matter of questionable technical character. However, since even with a narrow construction the claimed subject-matter does not involve an inventive step (see below), the Board will not pursue this possible objection.

3. *Inventive step*

3.1 As indicated in the Board's communication (see point VIII above), the Board judges that it would have been obvious for the skilled person, when starting from the appellant's closest prior art (ie the network management system illustrated in Fig. 1 of the application), to use a compartmented operating system. It would have been clear to him that there was a need for isolating users of shared network management systems. The application in fact mentions as a known requirement that "the operations systems have to be tightly controlled so that security, in terms of information flow control, is maintained" and describes previous efforts to achieve separation between the operators (see paragraphs [0002] to [0006]). The skilled person was thus not faced with the task of recognising the technical problem, but of solving it. Compartmented operating systems were well known at the priority date, as acknowledged in the application (see point 1 above). It must have been clear to the skilled person that their properties made them suitable in

particular for isolating users of a network management system.

3.2 Furthermore, the examining division held that the invention according to claim 1 (in the version before it) did not involve an inventive step when D1 was taken as a starting point (see point III above). In spite of the appellant's counterarguments set out in the statement setting out the grounds of appeal (see point V above), the Board agrees with the view taken by the examining division for the reasons given in the Board's communication (see point VII above).

3.3 It follows that the subject-matter of claim 1 does not involve an inventive step (Article 56 EPC 1973).

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

T. Buschek S. Steinbrener