BESCHWERDEKAMMERN
DES EUROPÄISCHEN
PATENTAMTS

BOARDS OF APPEAL OF
THE EUROPEAN PATENT
OFFICE

CHAMBRES DE RECOURS
DE L'OFFICE EUROPÉEN
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 26 September 2014

Case Number:	T 2267/13 - 3.5.01
Application Number:	07708802.9
Publication Number:	2002346
IPC:	G06F15/00
Language of the proceedings:	EN

Title of invention:
APPARATUS AND METHOD FOR USING INFORMATION ON MALICIOUS APPLICATION BEHAVIORS AMONG DEVICES

Applicant:
Samsung Electronics Co., Ltd.

Headword:
Malicious Behaviour/SAMSUNG

Relevant legal provisions:
EPC Art. 54(2), 123(2), 84

Keyword:
Novelty - (no)
Amendments - added subject-matter (yes)
Claims - clarity (no)

This datasheet is not part of the Decision.
It can be changed at any time and without notice.

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern
Boards of Appeal
Chambres de recours

European Patent Office
D-80298 MUNICH
GERMANY
Tel. +49 (0) 89 2399-0
Fax +49 (0) 89 2399-4465

Case Number: T 2267/13 - 3.5.01

DECISION
of Technical Board of Appeal 3.5.01
of 26 September 2014

Appellant:
(Applicant)

Samsung Electronics Co., Ltd.
129, Samsung-ro
Yeongtong-gu
Suwon-si, Gyeonggi-do, 443-742 (KR)

Representative:

D'Halleweyn, Nele Veerle Trees Gertrudis
Arnold & Siedsma
Bezuidenhoutseweg 57
2594 AC The Hague (NL)

Decision under appeal:

Decision of the Examining Division of the European Patent Office posted on 31 May 2013 refusing European patent application No. 07708802.9 pursuant to Article 97(2) EPC.

Composition of the Board:

Chairman S. Wibergh
Members: P. Scriven
P. Schmitz

Summary of Facts and Submissions

I. The appeal is against the Examining Division's decision to refuse European patent application 07708802.9. The Examining Division found that the claimed invention lacked novelty over document D1 (US-A1 2004/0143749).

II. The appellant, in the notice of appeal, requested that the decision be set aside and that a patent be granted on the basis of the main and auxiliary requests to be filed with the statement setting out the grounds of appeal. With that statement, the appellant filed a new main and two new auxiliary requests. Oral proceedings were requested, if the grant of a patent was not envisaged.

III. The Board arranged oral proceedings. In a communication sent with the summons, the Board set out its provisional view. In particular, the Board noted that D1 seemed to disclose the whole subject matter of claim 1 according to the main request and according to the second auxiliary request, and that the term "sharing directly", used in the first auxiliary request was unclear and lacked any clear basis in the application as filed.

IV. The appellant responded by letter dated 21 July 2014, with which a main and four auxiliary requests were filed.

V. In a further letter, dated 6 August 2014, the appellant's representative informed the Board that he would not attend the oral proceedings.

VI. Oral proceedings were held as scheduled on 26 September 2014. The appellant was not represented. The appellant's requests were that the decision under appeal be set aside and that a patent be granted on the basis of the main request or any of auxiliary requests 1 to 4, all filed with letter dated 21 July 2014.

VII. Claim 1 according to the main request reads as follows:

A device for using information on malicious application behaviors, the device comprising:
a capability-monitoring unit (210) that monitors application capabilities;
a behavior-monitoring unit (220) that monitors application behaviors;
an document generating unit that generates a document specifying the application capabilities and the application behaviors; and
a controlling unit that controls execution of an application using the generated document in the formal language,
characterized
in that the document generating unit is an mBDL-generating unit that generates a document in a formal language specifying the application capabilities and the application behaviors; and
by a network-administering unit that shares the document in the formal language, which is generated in the mBDL-generating unit, with other computing devices in an authenticated and trusted group, which other devices are susceptible to harmful functions generated by running the same malicious application.

VIII. Claim 1 according to the first auxiliary request reads identically except for the final clause (emphasis added):

...
by a network-administering unit that shares the document in the formal language, which is generated in the mBDL-generating unit, ***directly*** *with other computing devices in an authenticated and trusted group, which*

other devices are susceptible to harmful functions generated by running the same malicious application.

IX. Claim 1 according to the second auxiliary request reads as that according to the main request, except as follows:

...
a controlling unit that controls execution of an application using ***a document specifying the application capabilities and the application behaviors in a formal language,***
...
by a network-administering unit that shares the document in the formal language, which is generated in the mBDL-generating unit, ***(directly)*** *with other computing devices in an authenticated and trusted group, which other devices are susceptible to harmful functions generated by running the same malicious application,*
wherein the controlling unit is configured to control execution of an application using a shared document.

X. Claim 1 according to the third auxiliary request reads as according to the second auxiliary request, except that the following is appended:

...
and the devices have a function to parse the generated document in the formal language.

XI. Claim 1 according to the fourth auxiliary request reads as follows:

A device for using information on malicious application behaviors, the device comprising:
a behavior-monitoring unit (220) that monitors application behaviors;

an document generating unit that generates a document specifying the application behaviors; and

a controlling unit that controls execution of an application using a document specifying the application behaviors,

characterized

by a capability-monitoring unit (210) that monitors application capabilities;

in that the document generating unit is an mBDL-generating unit that generates a document in a formal language, additionally specifying the application capabilities;

in that the controlling unit controls execution of an application using the document specifying the application capabilities and the application behaviors in the formal language; and

by a network-administering unit that shares the document in the formal language, which is generated in the mBDL-generating unit, (directly) with a plurality of other user devices having different platforms in an authenticated and trusted group, which other user devices having different platforms are susceptible to harmful functions generated by running the same malicious application,

wherein the mBDL-generating unit generates the document in a formal language and specifying the application capabilities and the application behaviors in a common document form for sharing with the other user devices having different platforms, to enable the other user devices having the different platforms to parse the generated document in the formal language and wherein the controlling unit is configured to control execution of an application using a shared document.

XII. The appellant's arguments can be summarised as follows:

In prior-art methods of monitoring behaviour, in particular in D1, documents were shared via a server under the control of an anti-virus vendor. The invention was different, in that documents were shared between user-devices. Whereas the prior art required other devices to be running software from the anti-virus vendor, the invention did not. Nothing in the prior art suggested that end users should share documents amongst themselves. The Examining Division erred by considering that there was no technical difference between servers and user-devices, because, in the system envisaged according to the invention, user-devices had to be able to transmit and receive to and from each other, rather than being able only to transmit and receive to and from a server. Sharing between end users had the technical benefit of reducing network load.

The fact that claim 1 according to the main request defined a device in terms of the vulnerabilities of other devices was not a problem, because the device would sometime itself be one of the devices receiving a document.

A basis for direct sharing with a plurality of user devices could be found in Figure 7 and the corresponding description.

Regarding the second auxiliary request, the fact that the control unit of the claimed device based the execution of an application on the content of a shared document implied that this document had been generated and transmitted by some other device.

Regarding the third auxiliary request, the fact that the devices with which documents were shared were capable of parsing implied that the device which did the sharing was also capable of it.

In the fourth auxiliary request, the devices were explicitly defined as user devices. In addition, D1 disclosed only the generation of a log, but not of any capabilities of a potentially-malicious application. The fact that, in this request, the other devices were defined as having different platforms emphasized the difficulty of directly sharing documents. That difficultly was overcome by using a document in a common form.

Reasons for the Decision

Background

1. The invention concerns computer malware. One way of mitigating the effects of malware is to scan files to see if they contain the signature of a known virus, and taking some action if such a signature is found. The problem with that is that it relies on knowledge of the virus. It cannot identify files infected by some unknown virus.

2. The invention, therefore, takes a different approach. It monitors the behaviour of programs as they run. A program that behaves in a way it ought not to behave can be identified as a possible threat. One possible response is to prevent the program running.

3. This approach of monitoring behaviour was known before the priority date of the present application, as the appellant's arguments concede. D1 discloses an example it calls "APPFIRE": "[it] defines appropriate behavior based on the intended use of an application. If the

application exhibits inappropriate behavior for any reason, APPFIRE will prevent it" (D1, paragraph [0044]).

4. There is a further problem faced by systems based on observing behaviour. It is the question of how different machines come to know which behaviours are appropriate, and which are not. The present invention deals with that by producing a document specifying capabilities and behaviours, and by sharing such documents with an authenticated and trusted group.

5. The appellant accepts that, according to D1, a document specifying behaviour is produced and distributed, but argues that the nature of the document and its manner of distribution, are different.

The main request

6. Claim 1 according to this request is identical to that according to the main request submitted with the statement setting out the grounds of appeal.

7. The device defined by claim 1 comprises a unit that monitors the capabilities of applications, a unit that monitors their behaviours, a unit that generates a document specifying the capabilities and behaviours in some formal language, a unit that uses the document to control the execution of an application, and a unit that shares the document with other devices.

8. D1 discloses each of these units:

Units that monitor behaviour and capabilities.
The fundamental idea behind the system disclosed in D1

is that behaviour is monitored (D1, title, paragraphs [0053], [0055], [0080], [0081], for example). A program cannot behave in a way it is not capable of. Thus, in a trivial way, monitoring behaviour counts as monitoring capabilities. The Board recognises that the appellant seeks to draw a distinction between the two concepts, but neither the claim nor the description gives the terms "capability" or "behaviour" any meaning other than the normal English one. Thus, by watching behaviour, we see what a program is doing and at least some of what it is capable of doing.

A unit that generates a document.
D1 discloses the generation of several documents that describe behaviour (and therefore capabilities): the "behavior control description", (D1, paragraph [0052]) is one, and the "configuration" that can be "read and enforced" by agents and which can come from "trusted sources" or an "application itself" (D1, paragraph [0054]) is another. The Examining Division pointed to the profiler that "generates an initial BCD", and the Board notes that this initial BCD need not be generated by the vendor, but "can be used by customers to generate BCDs for their own custom applications" (D1, paragraphs [0204] and [0205]). The Board agrees that this is a document that describes behaviour and capabilities and that it is, sometimes at least, generated in the agent itself. Claim 1 defines this unit as "an mBDL generating unit that generates a document in a formal language." This says no more than that the document is in a machine-readable form, the form being suitable for describing malicious behaviour. The Board is satisfied that the "initial BCD" disclosed by D1 is such a document.
A unit that shares the document with other devices.
The Board understands that this unit makes a document

describing behaviour available to other devices. It may transmit the document, or simply allows other devices to access it. According to the claim, the sharing is with, at least, authenticated and trusted devices that are susceptible to harmful functions.
D1 discloses the reception of behaviour control descriptions and configuration information by agents, and the transmission of logs by them (D1, paragraphs [0087] - [0089], [0105], and [0106]). Of the items of data that can be transmitted, according to D1, the "configuration or log data" are relevant here (D1, paragraph [0090]). Thus, the appellant's argument that the agent only transmits log data is not substantiated. The configuration data mentioned above (D1, paragraph [0054]) is also transmitted. That is sufficient to disclose the unit that shares the document, in particular because it is transmitted to the "authenticated Management Infrastructure". It is inherent in D1 that harmful functions may affect other devices. That is why configuration data are sent to the various devices. That constitutes sharing with devices susceptible to harm.

9. The appellant's arguments that documents are shared between end users is not relevant to this claim. It is sufficient that the document is shared within an authenticated and trusted group. Nor does the Board see any relevance in the arguments that the system disclosed in D1 requires the agent to run software from an anti-virus vendor or that there is a distinction to be drawn between servers and user-devices.

10. The Board, therefore, considers that the disclosure of D1 anticipates the device defined by claim 1. The lack of novelty (Article 54 EPC) means that the main request

cannot be allowed.

11. Moreover, claim 1 seeks to define a device in terms of a property of other devices, namely of the group of devices with which the document is shared. These devices have to be "authenticated and trusted" and "susceptible to harmful functions." This seems to amount to an effort to define a device in terms of how it is used, rather than in terms of the device itself, and thus causes some unclarity.

The first auxiliary request

12. Claim 1 differs from that according to the main request in that the sharing is done "directly".

13. The application as filed does not mention direct sharing. In particular, the description of Figure 7, to which the appellant has pointed, does not mention it.

14. Figure 7 itself shows three connections, each between a device 910 and a less powerful device 904, 906, and 908. There is no requirement that the connections be direct. Indeed, the final sentence of paragraph [55] of the published application says that "devices 904, 906, and 908 can prevent the malicious applications from running by generating an mBDL document ... and sharing it with other devices." If the sharing is with any other device than 910, such sharing must pass through device 910. Any direct sharing seems to be precluded.

15. The appellant has not pointed to any other embodiment than that of Figure 7 as a possible basis, and the Board does not see any.

16. In addition, the Board is not satisfied that the terms "directly" has a clear meaning. Transmissions between nodes of a network (e.g. the Internet) normally pass through intermediate nodes. It is not clear whether the appellant seeks to exclude such intermediate nodes or has something else in mind, such as "directly" in the sense of "without delay" or "as soon as available".

17. The Board, is, therefore, satisfied that this version of claim 1 is unclear (Article 84 EPC) and cannot be allowed.

The second auxiliary request

18. Claim 1 differs from that according to the main request essentially in that the controlling unit uses "a document specifying capabilities" and "a shared document" rather than "the generated document" which specifies capabilities and behaviour.

19. Thus, the device defined by this claim is somewhat broader than in the main request. The same analysis, therefore, applies.

20. The appellant's argument that control was based on a shared document, which implied the document had been received from a different device, cannot be accepted. If device A shares a document, so that, say device B receives it or otherwise has access to it, then the document is a shared document. There is nothing odd about device A using the document it has shared with B. However, the Board also notes that D1 discloses both control based on a document received from another device and control based on a document generated in the device itself. Thus, the argument would not help the

appellant to establish novelty, even if it could be accepted.

21. Thus, the Board considers that this request cannot be allowed due to a lack of novelty (Article 54 EPC).

The third auxiliary request

22. Claim 1 according to this request differs from that according to the second auxiliary request in that the other devices, those with which a document is shared, are able to parse the document.

23. In the Board's view, when a document is transmitted in D1, it is implicit (at least) that the receiving device can read it, that is, parse it. This feature does not seem to add anything novel. Accordingly, this request cannot be allowed for lack of novelty (Article 54 EPC).

24. In addition, this feature does not characterise the device claim 1 seeks to define. It characterises other devices. It is unclear whether there is any limitation on the device itself, or, if there is, what limitation it might be.

The fourth auxiliary request

25. Claim 1 according to this request has been considerably re-drafted. However, apart from a different distribution of features to pre and post-charactering parts, the salient difference over the third auxiliary request lies in the stipulation that the other devices are user devices.

26. The term "user device" is not used in the application as filed. The nearest term is "user computer", but that is used only in paragraphs [0012] and [0013] of the published application, which refer to a prior art system. The application as a whole makes no mention of the devices in question being user devices.

27. The Board, therefore, considers that this version of claim 1 extends beyond the content of the application as filed (Article 123(2) EPC).

28. In addition, the lack of clarity noted with respect to the third auxiliary request applies equally to the fourth, and the reference to user devices is a further attempt at defining one device in terms of properties of other devices. It does not result in a clear definition of the claimed device.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

Beschwerdekammern des Europäischen Patentamts
Boards of Appeal of the European Patent Office
Chambres de recours de l'Office européen des brevets

B. ter Heijden S. Wibergh

Decision electronically authenticated