Internal distribution code:

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

Datasheet for the decision of 8 May 2019

Case Number: T 1882/17 - 3.5.06

Application Number: 13713630.5

Publication Number: 2828789

IPC: G06F21/56, G06F21/55

Language of the proceedings: EN

Title of invention:
COMPUTING DEVICE TO DETECT MALWARE

Applicant:
Qualcomm Incorporated

Headword:
Malware detection/QUALCOMM

Relevant legal provisions:
EPC Art. 56, 84

Keyword:
Claims clarity (no)
Inventive step (no)

Decisions cited:

Catchword:

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Case Number: T 1882/17 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 8 May 2019

Appellant: (Applicant)	Qualcomm Incorporated 5775 Morehouse Drive San Diego, CA 92121 (US)
Representative:	Bentall, Mark James Reddie & Grose LLP The White Chapel Building 10 Whitechapel High Street London E1 8QS (GB)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 1 March 2017 refusing European patent application No. 13713630.5 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	W. Sekretaruk
Members:	M. Müller
	G. Zucka

Summary of Facts and Submissions

I. The appeal is against the decision of the examining division to refuse, with reasons dated 1 March 2017, European patent application No. 13 713 630. Reference was made to documents

D1: US 2004/187023 A1,
D2: US 2007/074289 A1, and
D3: US 2011/055925 A1,

and it was found that the independent claims of then main and auxiliary requests 1 and 2 lacked inventive step over D1 in view of D2 and D3. An auxiliary request 3 was not admitted pursuant to Rule 137(3) EPC.

II. Notice of appeal was filed on 28 April 2017, the appeal fee being paid on the same day. A statement of grounds of appeal was received on 11 July 2017. The appellant requested that the decision be set aside and a patent be granted on the basis of claims 1-14, 1-14, 1-13 according to a main or one of two auxiliary requests, respectively.

III. In an annex to a summons to oral proceedings, the board informed the appellant of its preliminary opinion that the claimed invention lacked clarity and inventive step, Articles 84 and 56 EPC. Objections under Article 83 and 123(2) EPC were also raised.

IV. In response, the appellant did not file arguments or amendments but, with letter dated 4 April 2019, withdrew its request for oral proceedings and informed the board that no one would be attending the scheduled oral proceedings.

V. The oral proceedings were then cancelled.

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

"A method for a mobile computing device,
characterized in that
the method analyzes applications operating on the mobile computer device (102), the method comprising:
logging actions (220, 222, 320) for each of a plurality of applications (160, 162, 164, 166) in a log of actions (120);
generating a behavior vector (130) for each application of the plurality of applications based on the actions (220, 222, 320) recorded in the log of actions (120) including at least one behavior vector (130) that characterizes a behavior of its associated application via a plurality of numerical values based at least in part on a number (550) of user interaction events that occurred before the application was installed on the mobile computing device; and
classifying each application as benign or not benign based on the respective behavior vector (130)."

Claim 1 of auxiliary request 1 differs from that of the main request in that it is now specified that the behavior vector characterizes a behavior of its associated application not based on "events that occurred before" installation but

"... based at least in part on a number (5629 of SMS messages sent by the mobile computing device; ..."

Claim 1 of auxiliary request 2 reads as follows:

"A method for a mobile computing device,

characterized in that

the method analyzes applications operating on the mobile computer device (102), the method comprising:

logging, by a processor of the mobile computing device, actions (220, 222, 320) for each of a plurality of applications (160, 162, 164, 166) in a log of actions (120);

using, by the processor, a behavior analysis engine to generate a behavior vector (130) for each application of the plurality of applications based on the actions (220, 222, 320) recorded in the log of actions (120) including at least one behavior vector (130) that characterizes a behavior of its associated application;

using, by the processor, a classifier to determine whether the behavior characterized by each behavior vector for each application is benign or not benign based on the plurality of numerical values of the behavior vector; and

sending behavior vectors to a server and receiving updates for the behavior analysis engine, the updates for the behavior analysis engine being based on behavior vectors uploaded from a plurality of mobile computing devices."

Reasons for the Decision

The invention

1. The invention generally relates to malware detection. It is explained that traditional signature-based methods are deficient because they are computationally very demanding for known malware, even prohibitively so for mobile devices, and do not work for unknown malware

(see paragraph 4; all references herein are to the application as originally filed). The invention is meant to be "less processor and memory intensive" and to enable a quicker malware detection (paragraph 5).

1.1 The general architecture of the proposed system is depicted in figure 1 and summarized in paragraph 15. A "query logger" (108) running on a computing device (102) may generate a "log of actions" (120), from which, per application, a behavior vector (130) is created meant to "characterize" the behavior of the application. Via its behavior vector, each application is then classified (132) as either "benign" (140) or as "malware" (150).

1.2 Various types of actions may be logged, including, for example, "user interaction" and resource usage as well as frequency and timing (see paragraphs 29 and 32, and figures 2-5).

1.3 Per type of application (e.g. youtube, game, notepad, etc.) it is (pre-)defined which behavior is considered "normal" and thus benign. For example, a benign "youtube application" will have frequent user interface actions but no phone actions (see paragraph 37), whereas a deviation from this may indicate a "fake youtube application" (see paragraph 38).

1.4 It is then explained that a server may be provided which, like the clients, is equipped with a behavior analysis engine and a classifier, in the case of the server referred to as a "global classifier" (see paragraph 40, in particular lines 5-7, and figure 6, in particular nos. 622, 626 and 628). The server will "aggregate behavior reports" from multiple devices (paragraph 40, lines 1-3) and, on this basis, update

the global classifier (paragraph 41). For instance, if a client has found an application to be suspicious, the server may be asked to classify that application as benign or malicious (see paragraphs 42 and 48, figure 6). Moreover, the server may transmit an "update" for "the behavior analysis engines" or the "queries" - and, in general, the "behavior models" - on the individual mobile devices (see, e.g., paragraphs 43, 49 and 50, and figure 6, the arrows emanating upwards from box no. 622).

1.5 The behavior analysis engine and classifier in question are said to be initialized based on "known-bad" and "known-good" applications and trained using "standard supervised machine learning techniques" (paragraph 51). Classification is based on "similarity" with known malware or benign applications (paragraph 52).

1.6 The independent claims of the main request specify that the behavior vector depends "at least in part on a number [...] of user interaction events that occurred before the application was installed". This is disclosed in paragraph 27 of the description. The independent claims of auxiliary request 1 specify that the behavior vector depends "at least in part on a number [...] of SMS messages sent" by the device. This is disclosed in paragraph 26. The independent claims of auxiliary request 2 focus on the server to which behavior vectors are sent and from which "updates for the [local] behavior analysis engine" are received.

Clarity, Article 84 EPC, and claim construction

2. The claims use some very broad terminology, the precise scope of which must be determined before inventive step

can be properly assessed. Some of the claim language turns out to be unclear.

2.1 The claimed "log of actions" is a collection of entries for each of the logged actions of interest. It is not specified which action parameters precisely are "logged".

2.2 The "behavior vector" is a collection of "numerical values" which is generated from the log of actions and, as a whole, "characterizes a behavior". No detail is claimed as to how many values are contained in a vector, from what range they are taken or how, in general, the behavior vector is to "characterize" behavior.

2.3 It is also not defined in any detail how the applications are classified as "benign or not benign" based on the behavior vector.

2.4 Regarding the central feature of the main request "number of user interaction events that occurred before the application was installed": It is not defined which user events are counted or how long "before" the installation they are taken into account. The board considers that both issues render this feature unclear, Article 84 EPC.

2.5 As regards auxiliary request 2, the board notes that the claims specify that the updates received are "for the behavior analysis engine", not "of" as the appellant seems to imply (see grounds of appeal, page 17, point 4).

2.6 More importantly, though, the claims of auxiliary request 2 do not specify how the "updates" are meant to

affect the behavior analysis engine. The description states that the "behavior analysis engine and classifier" are trained (see paragraph 51). While the board considers known the idea of training a classifier, in the present case the mapping of behavior vectors to the finding that an application is benign or not benign (see figure 1, nos. 132, 140 and 150), it is not clear what "training" or "updating" the behavior analysis *engine* involves, nor how such updates are determined. The description also refers to the "behavior model" which may have to be updated, but does not define what this "behavior model" is that is "push[ed] to the behavior analysis engine" (see e.g. paragraph 53). As a consequence, the board considers that the claimed "updates for the behavior analysis engine" render the claims of auxiliary request 2 unclear, Article 84 EPC.

2.7 Further with regard to auxiliary request 2 it is noted that the claimed individual mobile device is not limited by how the "updates" are computed at the server, in particular not by the fact that there are further mobile devices involved. For that reason, too, the independent claims of auxiliary request 2 are unclear, Article 84 EPC.

The prior art

3. D1 discloses a malware detection system (see figure 3) which monitors *inter alia* "process behavior information" (see figure 2 and paragraphs 34 and 37).

3.1 A "malicious code detection program" including "detection routines" (see figure 2, nos. 42, 52 and 54, v1-vm and t1-tm) may operate "on an as-needed basis, a periodic basis, a random basis" or "an event driven

basis" (see paragraph 35). For instance, if a program is detected to log keystrokes, this may indicate that it is malicious (paragraph 39). Individual indicators that a program is benign ("valid") or malicious are "weighted" and combined so as to produce a "valid program score" and a malicious code score (see figure 2 and paragraphs 41 to 44). Based on thresholding the two scores (V_{thres}, T_{thres}) and comparing them with each other, it is decided whether the program is valid, malicious or suspicious (see paragraphs 50 and 51).

3.2 The security software runs locally on each client machine, for instance as an Internet browser plugin (see figure 3 and paragraph 66). D1 focuses on using the malware detection to protect online transactions with various companies (see paragraph 108). The companies may automatically distribute their respective security software to potential clients, "before, during and/or after an online transaction" (paragraphs 30 and 111).

4. D2 also discloses a centralised malware detection system based on event tracking and activity analysis of the programs in question. Clients regularly send log files to a host and receive weights adapted in view of the reports from several computers (see e.g. paragraphs 24 and 28, and figures 2 and 3, in particular nos. 316, 320, 322-330, 336 and 338).

5. D3 discloses a centralised (server-based) system for assessing ("auditing") the security posture of client machines. Client machines create "security reports" including "security events" that have occurred and/or "security states" of the machine: This may include information on whether an executable file was installed or a wireless connection was made, and how often, or

configuration parameters of the client machine such as time zone, geographical location, platform etc. It is also disclosed that "an event following installation of a client application" or "following refusal by the user to install the client application" may be detected as relevant (see paragraphs 11-26 and 125, and claim 9). An "audit server" then searches for "patterns" in the report, e.g. by detecting that the frequency of certain actions is considerably more frequent than "normal" or that installations take place at irregular times of day (see paragraphs 34 and 101 *et seq.*). What is considered "normal" or not may depend on the type of application (see figures 8A to 8D).

Inventive step, Article 56 EPC

Main request

6. The examining division has based its assessment of inventive step on document D1, the board regards this as a suitable choice and the appellant has not challenged it.

6.1 The valid and malicious code detection routines of D1 (see figure 2) gather "behavior information" by analysing, *inter alia*, a table of network connection activities, see paragraph 38) or whether a program is logging keystrokes (paragraph 39). In the board's view, this implies a "log of actions" within the meaning of the present claims. Detection routines may output numerical values (paragraph 39). The totality of these numbers can be considered a "behavior vector" on the basis of which the decision "benign or not" is made.

6.2 Thus the board agrees with the finding in the decision that the only difference between claim 1 of the main

request and D1 is that "the number of user actions before installation" is taken into account for that decision. Also the appellant does not challenge this analysis. Although it states that claim 1 and D1 differ by "at least" this feature (see grounds of appeal, page 3, paragraph 5), it does not mention any other difference specifically.

7. The examining division found that "there [was] no apparent special technical effect of using this specific factor" and that, hence, this feature had to be "considered as merely a selection of a factor [...] which as such is not inventive" (see reasons 1.2). The board understands this argument as saying that the selection of an arbitrary, further factor cannot support the presence of an inventive step, and agrees with it.

7.1 In its full breadth, the feature is satisfied by counting all kinds of "user interactions", which *prima facie* have nothing to do with the question of whether the application being installed is benign or not. Not only is it not defined (in the claims or the description) *how* the number of user actions before installation contributes to the decision whether an application is benign or not, it is not even made plausible *that* the feature in its full breadth can contribute to this decision.

7.2 Therefore, the board is not convinced that the feature in its full breadth can be said to contribute to the effect of classifying an application as benign or not, and which other effect - technical or not - it may have is unclear. The board concludes that the feature cannot establish an inventive step, Article 56 EPC.

8. The appellant argues that the skilled person would "appreciate" the importance of that criterion because "applications installing themselves with zero or minimal user interaction might not be desired by the user". The appellant also states that it is "background knowledge" that computer viruses may show this undesired behavior. The skilled person would also "deduce from the application" that the feature had to be "helpful", because otherwise "it would not be mentioned in the application". The board considers that this argument rather indicates lack of inventive step. If the skilled person were assumed to know that viruses may install themselves with little user interaction, it would follow immediately that user interaction before installation could be an indicator for virus detection. The skilled person wanting to improve D1 would thus not hesitate to incorporate this additional indicator and, thereby, arrive at the subject-matter of claim 1 without an inventive step, Article 56 EPC.

9. For this finding, a reference to D3 is not necessary. However, for completeness' sake, the board considers that the skilled person would always try to improve the system of D1 by incorporating further classification criteria.

9.1 In doing so, the skilled person would, in the board's view, come across D3. In this regard, it is immaterial whether D3 is common general knowledge - which, by the way, the ED did not state (see the decision, reasons 1.3, and the grounds of appeal, page 4, point 2).

9.2 D3 discloses that events "following installation" of a client application (see e.g. paragraph 26) or "following refusal by the user to install the client application" may be relevant. More generally, "several

concurrent dimensions of characteristics that are used to describe an installation or execution of an application" may be taken into account (see paragraph 125). In the board's view, the skilled person considering what might "describe an installation" would obviously think of what the user did to effect the installation and thus consider, without exercising an inventive step, the number of user interactions before installation.

9.3 The board also does not think that it would distort the teaching of D3 to consider the incorporation of individual "criteria" disclosed in (or suggested by) D3 into D1 (see the grounds of appeal, page 6, paragraph 9), because the skilled person would, at times, look precisely for additional criteria in order to improve the system of D1. But even if the appellant were right that the skilled person would not want to incorporate any new criterion from D1 without also incorporating a centralized server (see the grounds of appeal, page 7, paragraph 4), this argument would not establish the appellant's case: The board cannot see that D1 would be incompatible with a solution in which, say, the individual companies' servers would cooperate with the locally installed security software, and also claim 1 of the main request does not exclude that the behavior vector is analysed with the help of a server (see the grounds of appeal, page 8, paragraph 3).

10. For the above reasons, the board finds that the independent claims of the main request lack an inventive step over D1, in view of common general knowledge or in view of D3, Article 56 EPC.

Auxiliary request 1

11. Similarly to point 8 above, the board agrees with the decision that the specific impact of the "number of SMS messages" for malware detection is not claimed and that, hence, this criterion may be viewed as a merely arbitrary selection of a further "factor" which cannot establish inventive step, Article 56 EPC. The board also notes that, even if the skilled person might be able to "deduce" that a particular feature must be "helpful" or advantageous because it is mentioned in the application (see the grounds of appeal, page 10, last paragraph), this insight alone is not sufficient to enable the skilled person to also determine "how" the feature is helpful and thus which specific (technical) effect it has. The insight alone also cannot overcome a lack of essential feature of the independent claims.

12. D3 proposes in paragraph 102 the analysis of whether an application is installed on "friend invitations or messages from friends" and paragraph 103 suggests a correlation of this criterion with "malware spreading through SMS" (see also paragraph 105). This primarily relates to an SMS received at the local device before installation rather than, as claimed, the SMS sent from the device. Also paragraph 106 relates to the "history of an application installation", i.e to what happened before and not after installation. However, paragraph 107 refers to the fact that malware may "use the user's address book" in order to spread, which, in the board's understanding, relates to what a malicious application may do after installation in order to "spread" further. Hence, the board agrees with the examining division - and disagrees with the appellant (see the grounds of appeal, page 12, paragraphs 1-5) that D3 suggests the

relevance of SMS sent from the infected device to identify an application as malicious or not. The independent claims of auxiliary request 1 thus also lack inventive step over D1 and D3, Article 56 EPC.

Auxiliary request 2

13. Under the proviso of the above-mentioned deficiencies under Article 84 EPC, the board takes the following position on inventive step.

13.1 As the board understands the claims of auxiliary request 2, a behavior analysis is always carried out locally at the mobile computing device, and the server is only used to modify the "behavior model" on the basis of "behavior vectors" generated at and obtained from several mobile devices.

13.2 The board considers it obvious that detection routines such as those of D1 may have to be modified, for instance so as to reflect new insights on existing malware. The board also considers it to be an obvious option to base any such modification, at least partially, on the data previously obtained, i.e. the behavior vectors. The board considers that it would be obvious not to carry out this modification at the mobile devices, for instance in order to reduce the computational load on them or because it may be desirable to involve an expert in the process of modifying the detection routines which is easier to realise at a server.

13.3 Therefore, the board takes the view that sending the behavior vectors to a server for consideration and receiving suitable "updates" is an obvious option for maintaining the accuracy and relevance of the detection

routines of D1 and that, hence, claim 1 of auxiliary request 2 lacks inventive step over D1 alone, Article 56 EPC.

14. The board however also agrees with the decision that the general idea of involving a server in updating the local "models" is known from D2 (see figure 2).

14.1 The appellant insists that D2 discloses the transmissions of the "log" rather than the results of the detection routines and the return of adapted weights rather than modified detection routines (see the grounds of appeal, page 14, paragraphs 6-10) so that a combination of D1 with D2 would still not yield the claimed invention.

14.2 On the understanding that a "log" is not numerical while a behavior vector is, the board accepts these distinctions. However, the board considers it as an obvious option in the context of D2 for the host not to analyse the "log" itself but a numerical behavior vector derived from and characterizing it. Whether or not such a behavior vector is sufficient to determine "patterns" of interest would seem to depend on unspecified details about the behavior model, i.e. the behavior vectors and how they characterize behavior. Also whether "weighted factors" are returned or decision routines depending on them, is, in the board's judgment, an obvious matter of programming convenience: It may, for instance, be simpler to provide adapted detection routines rather than to program suitably parameterized detection routines so that the mere transmission of numbers is sufficient to effect the desired change. Finally, the appellant claims a bandwidth reduction (see page 16, paragraph 8) which, however, the examining division questioned

(paragraph 9) and for which, nonetheless, the appellant has not provided any evidence.

14.3 The board thus concludes that the differences mentioned by the appellant could not establish an inventive step over D1 in view of D2, Article 56 EPC.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

N. Schneider W. Sekretaruk

Decision electronically authenticated