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 24 November 2015

Case Number:	T 2480/10 - 3.5.06
Application Number:	04822016.4
Publication Number:	1743228
IPC:	G06F1/00
Language of the proceedings:	EN

Title of invention:
METHODS AND SYSTEMS FOR COMPUTER SECURITY

Applicant:
Computer Associates Think, Inc.

Headword:
Unfamiliar software/COMPUTER ASSOCIATES THINK

Relevant legal provisions:
EPC 1973 Art. 56

Keyword:
Inventive step - (no)

Decisions cited:

Catchword:

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 2480/10 - 3.5.06

DECISION
of Technical Board of Appeal 3.5.06
of 24 November 2015

Appellant:
(Applicant)

Computer Associates Think, Inc.
One Computer Associates Plaza
Islandia, New York 11749 (US)

Representative:

Dunlop, Hugh Christopher
RGC Jenkins & Co.
26 Caxton Street
London SW1H 0RJ (GB)

Decision under appeal:

Decision of the Examining Division of the European Patent Office posted on 15 July 2010 refusing European patent application No. 04822016.4 pursuant to Article 97(2) EPC.

Composition of the Board:

Chairman	W. Sekretaruk
Members:	A. Teale
	G. Zucka

Summary of Facts and Submissions

I. The appeal is against the decision of the examining division, the reasons for which were dispatched on 15 July 2010, to refuse European patent application No. 04 822 016.4 on the basis of lack of inventive step, Article 56 EPC, of the main and first and second auxiliary requests in view of the following document:

D1: US 2003/0163510 A1

and common general knowledge.

II. A notice of appeal was received on 24 September 2010, the appeal fee being paid on the same day. The appellant requested that the decision be set aside and made an auxiliary request for oral proceedings.

III. With a statement of grounds of appeal, received on 24 November 2010, the appellant submitted a main and first and second auxiliary requests, the claims of which were the same as those of the main, second and first auxiliary requests, respectively, on which the appealed decision was based.

IV. The board issued a summons to oral proceedings, giving in an annex its preliminary opinion that D1 seemed to be insufficiently relevant to the claimed subject-matter to warrant further discussion. Instead, the board introduced the following document, cited in the International Search Report, in view of which none of the requests seemed to involve an inventive step, Article 56 EPC 1973:

D2: US 2004/0039921 A1.

V. With a letter dated 24 August 2015 the appellant submitted amended claims according to a first and a second auxiliary request and amended pages 4 and 5 of the description according to all requests.

VI. Oral proceedings were originally planned for 2 November 2015 but were postponed by the board under Article 15(2) RPBA in response to a fax from the appellant's representative on the morning of the oral proceedings stating that, due to adverse weather conditions in London on the day before the oral proceedings, his flight to Munich had been cancelled. Despite exhaustive efforts, it had not been possible to find an alternative flight.

VII. Oral proceedings were eventually held on 24 November 2015 during which the appellant filed a new second auxiliary request and requested that the decision under appeal be set aside and that a patent be granted on the basis of the following claims:

main request: 1 to 31, received on 24 November 2010,
first auxiliary request: 1 to 23, received on 24 August 2015,
second auxiliary request: 1 to 17, filed during said oral proceedings.

VIII. At the end of the oral proceedings the board announced its decision.

IX. The remaining application documents on file are as follows.

Description:
Pages 1 to 3 and 6 to 12, as published (all requests).
Page 4, received on 24 August 2015 (all requests).

Page 5, received on 24 August 2015 (main and first auxiliary requests).
Page 5, filed during said oral proceedings (second auxiliary request).

Drawings:
Sheets 1 and 3 to 5, as published.
Sheet 2, received on 27 December 2007.

X. Claim 1 of the main request reads as follows:

"A computer-implemented method for maintaining computer security, comprising: providing (S21) a database (303) of known good software; opening (S22, S30) a file; identifying (S23, S31) the file being opened; determining (S24, S32) whether an entry exists in the database (303) of known good software for the identified file; and performing (S26, S27) at least one of allowing and preventing the opening of the file from continuing based on the result of the determination, the method characterized by: providing a database (304) of unfamiliar software; determining (S35) whether an entry exists in the database (304) of unfamiliar software for the identified file if it is determined that an entry does not exist in the database (303) of known good software for the identified file; adding (S37) an entry to the database (304) of unfamiliar software if it is determined that an entry for the identified file does not exist in the database (304) of unfamiliar software; if it is determined that an entry for the identified file exists in the database (304) of unfamiliar software, determining (S38-S40), based on an amount of time that the entry has been in the database (304) of unfamiliar software or the number of times that the identified file has been opened, whether the entry in the database (304) of unfamiliar software can be moved to the database (303) of known good software; and selectively moving (S42) the entry from the database (304) of unfamiliar software to the database (303) of known good software based on the determination as to whether the entry can be moved to the database (303) of known good software."

The claims according to the main request also comprise an independent system claim 16 and an independent claim 31 for a computer recording medium including computer executable code.

XI. Claim 1 of the first auxiliary request reads as follows.

"A computer-implemented method for maintaining computer security, comprising: providing (S21) a database (303) of known good software that is known to not perform harmful actions; determining (S24, S32) whether an entry exists in the database (303) of known good software for an identified file; and allowing (S26, S27) the opening of the file to continue when it is determined that an entry exists in the database of known good software for the identified file; providing a database (304) of unfamiliar software; determining (S35) whether an entry exists in the database (304) of unfamiliar software for the identified file if it is determined that an entry does not exist in the database (303) of known good software for the identified file; adding (S37) an entry to the database (304) of unfamiliar software if it is determined that an entry for the identified file does not exist in the database (304) of unfamiliar software; the method characterised by: opening (S22, S30) a file; identifying (S23, S31) the file being opened; if it is determined that an entry for the identified file exists in the database

(304) of unfamiliar software: determining (S38-S40), based on an amount of time that the entry has been in the database (304) of unfamiliar software or the number of times that the identified file has been opened, whether the entry in the database (304) of unfamiliar software can be moved to the database (303) of known good software; selectively moving (S42) the entry from the database (304) of unfamiliar software to the database (303) of known good software based on the determination that the entry can be moved to the database (303) of known good software; and placing one or more operating system call hooks before continuing to open the file, including notifying a Trojan notification service and prompting the user for input about whether the operating system call should be passed along or fail."

The claims according to the first auxiliary request also comprise an independent system claim 12 and an independent claim 23 for a computer recording medium including computer executable code.

XII. Claim 1 of the second auxiliary request differs from claim 1 of the first auxiliary request in that the characterising part of the claim reads as follows (additions underlined, deletions ~~struck through~~):

"opening (S22, S30) an executable program file, the program file comprising at least one executable operating system instruction;
identifying (S23, S31) the program file being opened;
if it is determined that an entry for the identified program file exists in the database (304) of unfamiliar software:
determining (S38-S40), based on an amount of time that the entry has been in the database (304) of unfamiliar

software or the number of times that the identified program file has been ~~opened~~ executed, whether the entry in the database (304) of unfamiliar software can be moved to the database (303) of known good software; when it is determined that the entry can be moved to the database (303) of known good software: selectively moving (S42) the entry from the database (304) of unfamiliar software to the database (303) of known good software ~~based on the determination that the entry can be moved to the database (303) of known good software~~ and allowing the system to continue to open and execute the program file; and
when it is determined that the entry cannot be moved to the database (303) of known good software: monitoring the execution of the program file for suspicious activity by placing one or more operating system call hooks corresponding to the at least one executable operating system instruction before allowing the system to ~~continuing~~ continue to open and execute the program file, wherein when a call hook occurs, the execution of the program file is halted until it is granted permission to proceed ~~including notifying a Trojan notification service and prompting the user for input about whether the operating system call should be passed along or fail~~."

The claims according to the second auxiliary request also comprise an independent system claim 9 and an independent claim 17 to a computer recording medium including computer executable code.

Reasons for the Decision

1. The admissibility of the appeal

The appeal fulfills the admissibility criteria under the EPC and is therefore admissible.

2. The context of the invention

2.1 The application relates to a malware protection method based on a database of "known good software" (303 in figure 3B) and a database of "unfamiliar software" (304 in figure 3B).

2.2 When a file is opened, a check is made of whether an entry exists for the file in the database of known good software (steps S30 to S33 in figure 3A). If so, then the operating system is allowed to continue opening and utilizing the contents of the file (step S34 in figure 3A; page 9, lines 11 to 19).

2.3 If such an entry does not exist, then the method checks the database of unfamiliar software for an entry (S35 in figure 3A; page 9, lines 19 to 22). The database of unfamiliar software includes time-stamp information for each entry indicating the creation time of the entry and the number of times each unfamiliar file or piece of software has been opened or executed (page 9, lines 6 to 10).

2.4 If an entry is not found in the database of unfamiliar software, then a new entry is created (page 9, line 22 to page 10, line 1).

2.5 If an entry is found in the database of unfamiliar software, and if its time-stamp indicates that the entry has been in the database for a "sufficient period of time" (for instance, a month or more) or the number of times the file has been opened exceeds a "baseline value", then the entry is moved to the database of known good software, and the operating system is thereafter allowed to open the file (S35, S36, S38, S39, S40 and S42 in figure 3A; page 10, lines 8 to 20).

2.6 If the entry is found in the database of unfamiliar software, but the entry has not been in the database for a sufficient period of time, or the number of times the file has been opened is less than the baseline value, then the operating system is allowed to open the file, but one or more operating system call hooks (305 in figures 3B and 4) are placed to notify a Trojan notification service which, in turn, prompts the user for input as to whether the operating system call should be passed on or fail (page 9, lines 2 to 5; page 10, lines 2 to 6; page 10, line 21, to page 11, line 21; figure 4).

3. The prior art

3.1 In the appealed decision D1 was considered to represent the closest prior art.

3.2 D1 discloses a method of administering user access rights to application programs on a computer system by means of a "list of allowed tasks for each user" (4 in figures 2 and 3), created on the basis of the user profile (6 in figure 2) in the "user database" (5 in figure 2) comprising user profiles indicating users' group memberships and function records (11 and 12 in figure 2; [0047] to [0049]) and a "database of tasks" (7 in figure 2) comprising task records ([0040] and [0041]).

3.3 The examining division, in the decision under appeal, considered the "list of allowed tasks for each user" in D1 to correspond to the database of known good software of the invention.

3.4 Given that D1 does not relate to malware protection, but rather to user access rights, and that the database of known good software of the invention is not meant to be a list of software that a user is authorised to execute, but a list of software that is known not to be malicious, the board does not consider D1 to be sufficiently relevant to the subject-matter of the invention to warrant further discussion. In the board's view, D2, cited in the International Search Report, but not relied upon in the examination procedure, is more relevant for the purposes of assessing the inventive step of the present invention.

3.5 D2 discloses a method of detecting rogue software. The method calculates fingerprints for all files relating to the operating system or application software used in a typical computer system ([0033]) using a cryptographic hash function ([0034] and [0035]) and creates a "database of acceptable file fingerprints" (16 in figure 1). The hash values calculated on a client computer (12 in figure 1) are transferred to a server (14 in figure 1) which compares them with the hash values in the database of acceptable file fingerprints ([0038]). If the hash results match, then the client program is regarded as being safe ([0039], [0040] and [0045)). Otherwise, if the database has no entry for such a file or if the hash value in the database entry for the file does not match the hash value received from the client, the file is determined to be possibly unsafe ([0039], [0041], [0042]). For such files the system administrator checks with the owners of the applications to verify the hash values ([0043]). All remaining questionable files are checked by the system administrator using additional management software and, if they are found to be acceptable, their hash values are stored in a second database ([0044], claim 6). By statistically comparing the hash of questionable files with hash values in the second database, the method can make heuristic guesses as to whether the received hash value is acceptable ([0047] to [0053], claims 7 and 8).

4. The main request

4.1 The board considers the "database of acceptable file fingerprints 16 which houses all the pre-calculated hash values for all files in various operating systems and applications" in D2, [0038] to be a "database of known good software" in the terms of claim 1. The method of D2, upon receiving hash values from the client, classifies files into three categories (see D2, [0040], [0041] and [0041]) of which the latter two are possibly unsafe. The board considers the list of possibly unsafe files in D2 [0039] to correspond to the "database of unfamiliar software" of the invention. Although the appellant has contested whether the list of possibly unsafe files in D2 can be regarded as the claimed "database of unfamiliar software", the appellant has not demonstrated any technical difference between the list known from D2 and the claimed "database".

4.2 Accordingly the subject-matter of claim 1 of the main request differs from the method known from D2 in that

i) it is executed when a file is opened (unlike D2 in which all files on a client computer are scanned) and

ii) potentially unsafe files (which are in the "database of unfamiliar software"), once a certain time has lapsed or a number of runs has been exceeded, are deemed to be safe (and moved to the "database of known good software").

4.3 Regarding difference (i), the board considers scanning a file when it is opened or at the request of a user, or scanning a whole computer at a particular time or on request to be well-known alternative scopes and schedules for running malware protection software. The appellant has not alleged that this feature involves an inventive step, and the board finds that it does not.

4.4 Regarding difference (ii), in the annex to the summons to oral proceedings the board expressed doubts as to whether this feature had an enhanced security effect, as the claim sets out neither the security analysis of unfamiliar software to establish whether it is harmful, nor the identification of aspects which make it harmful.

4.5 At the oral proceedings the appellant argued that this was a novel approach to structuring and maintaining databases without human intervention, based on tangible criteria implementing a trust factor. The appellant defined the objective technical problem solved by this difference as providing an improved tool for managing malware databases and argued that the inventive solution lay in the provision of technical criteria concerning activity associated with files for managing malware databases.

4.6 The board does not accept the appellant's formulation of the objective technical problem, as the invention does not provide any tool for database management in the sense commonly understood in the field of computing. In the view of the board, claim 1 of the main request provides rules for automated movement of entries from one database to another. The board does not consider this to be a technical contribution, as the classification of entries for files as "known good" or "unfamiliar" does not have a technical effect *per se*. In order to acknowledge the presence of an inventive step, a further technical effect of said classification, for example in terms of improved security, would have to be demonstrated. This the appellant has failed to do. The notion of security according to the invention is that, if no malicious activity of a particular piece of software has been observed over a certain period (defined either as a duration or as a number of times the software has been run), it can be trusted. However trust alone does not protect a computer system from a potentially malicious entity for which no malicious activity has yet been observed. Hence the board is not convinced that this difference has a technical effect.

4.7 The appellant has also argued, but then withdrew the argument in the oral proceedings, that the invention provides "zero-day protection", meaning that it protects a computer against attack from a piece of malware which cannot be detected by conventional anti-virus products, since they have not yet been updated with an appropriate signature; see page 4, lines 3 to 7, of the amended description. As the board explained in the oral proceedings, merely preventing unfamiliar software from running on a computer will not necessarily protect it from a zero-day vulnerability. As D2 states in paragraph [0002], malware on a computer may act over an extended period of time, without the user being aware that it is carrying out unauthorized activities.

4.8 Consequently the board finds that the subject-matter of claim 1 of the main request does not involve an inventive step, contrary to Article 56 EPC 1973.

5. The first auxiliary request

5.1 Editorial amendments aside, claim 1 of the first auxiliary request differs from that of the main request in that, if a file is "unfamiliar software", then one or more operating system call hooks are placed before continuing to open the file, a Trojan notification service is notified and the user is prompted for input as to whether the operating system call should be allowed.

5.2 The appellant argued at the oral proceedings that the first auxiliary request provided technical implementation details going beyond a mere classification of files and which were not disclosed in D2. In particular, D2 relied on an evaluation of file hash values and did not disclose or suggest any monitoring of operating system calls invoked by the file. Although the appellant accepted that hooking *per se* would have been well known to the skilled person, it argued that using hooking in the context of the invention and then prompting the user to allow the system call was not obvious. The appellant also explained that the "Trojan notification service" was a service to which suspicious files could be reported. It was referred to in the claim merely to emphasise the context. The ensuing actions of the "Trojan notification service" were not relevant.

5.3 The board finds that the problem solved by claim 1 of the first auxiliary request is maintaining computer security when opening unfamiliar software. The board does not consider the solution to be inventive. As the appellant has accepted, hooking is a standard programming technique. The board is not convinced by the appellant's argument that its use would not be obvious in the context of the present invention. Indeed the board sees no reason why this standard technique for monitoring program behaviour would not have been employed in the field of computer security. It would further have been obvious for the skilled person to hook operating system calls in particular, as invocations of operating system calls can potentially be more harmful than other activities of a computer program and thus worthy of closer monitoring. Prompting the user to either allow or confirm the execution of a task is moreover standard practice.

5.4 Thus the board finds that the subject-matter of claim 1 of the first auxiliary request does not involve an inventive step, contrary to Article 56 EPC 1973.

6. The second auxiliary request

6.1 Compared to claim 1 of the first auxiliary request, claim 1 of the second auxiliary request specifies explicitly that the file is an executable program file comprising at least one executable operating system instruction. These features are implicit in the claims according to the higher ranking requests, as the databases comprising the entries for the files are named "database of known good <u>software</u>" and "database of unfamiliar <u>software</u>" (emphases by the board).

6.2 Beyond that, claim 1 of the second auxiliary request clarifies the context and order in which the last two steps of the method of claim 1 of the first auxiliary request are executed. The step of moving the entry for the executable file to the database of known good software when the file is executed, is carried out if it is determined that the entry can be moved. The step of executing the file with operating system call hooks is carried out if it is determined that the entry cannot be moved. Although these conditions were not explicit in the wording of claim 1 of the first auxiliary request, the board's understanding of the invention and its resulting reading of claim 1 of the first auxiliary request in the light of the description already assumed the presence of these features.

6.3 Thus the board's assessment of claim 1 of the first auxiliary request also applies to claim 1 of the second auxiliary request.

6.4 Consequently the board finds that the subject-matter of claim 1 of the second auxiliary request does not involve an inventive step, contrary to Article 56 EPC 1973.

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. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated