Internal distribution code:

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

Datasheet for the decision of 30 April 2019

Case Number: T 1403/17 - 3.5.06

Application Number: 14180994.7

Publication Number: 2827273

IPC: G06F21/56, H04L29/06

Language of the proceedings: EN

Title of invention:
System and method for dynamic generation of anti-virus databases

Applicant:
Kaspersky Lab, ZAO

Headword:
Dynamic generation of anti-virus databases/KASPERSKY

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 1403/17 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 30 April 2019

Appellant: (Applicant)	Kaspersky Lab, ZAO 39A/3 Leningradskoe Shosse Moscow 125212 (RU)
Representative:	Sloboshanin, Sergej V. Füner Ebbinghaus Finck Hano Patentanwälte Mariahilfplatz 3 81541 München (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 8 February 2017 refusing European patent application No. 14180994.7 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, dated 8 February 2017, to refuse European patent application No. 14 180 994 for lack of inventive step over the document

D3: US 2011/047620 A1.

II. Notice of appeal was filed on 7 April 2017, the appeal fee being paid on the same day. A statement of grounds of appeal was received on 8 June 2017. The appellant requested that the decision be set aside and a patent be granted on the basis of claims 1-12 according to a main request or an auxiliary request as filed with the grounds of appeal.

III. In an annex to a summons to oral proceedings, the board informed the appellant of its preliminary opinion that the claimed invention lacked inventive step, Article 56 EPC. A few objections under Article 84 EPC were also made.

IV. In response to the summons, by letter dated 29 March 2019, the appellant filed amended claims 1-12 according to a main or an auxiliary request and amended description pages 1 and 2.

V. Oral proceedings were held on 30 April 2019, during which the appellant filed further amended claims 1-12 according to an auxiliary request 2. In view of this, the pending auxiliary request will be referred to as "auxiliary request 1".

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

"A computer-implemented system for dynamic generation of anti-virus (AV) databases, the system comprising a server (110) within a server-client environment, the server (110) comprising:

a server-side AV database (315) containing data related to known malware objects;

a request processing module (311) configured for receiving and processing user requests from a user computer (120-128, 210);

a user profile database (312), a data processing module (313), and a server update module (316),

characterized by

the request processing module (311) configured to insert user data upon initial user registration of the user computer (120-128, 210) into the user profile database (312) and to inform the data processing module (313) about the received user data for generating a user-side AV database (216) for the user computer (120-128, 210) using the server-side AV database (315) and the user data, wherein the user data comprises user parameters collected for registration that include a user ID, a user geographical location, an AV application version, an AV database version, visited site statistics and detected malware object statistics;

the server update module (316) configured to send the generated user-side AV database (216) to the user computer (120-128, 210);

the user profile database (312) connected to the request processing module (311), the user profile database (312) containing the user parameters, and subsequent parameter changes that are inserted into the user profile database (312) by the request processing module (311);

a forced update module (317) configured for sending a notification upon an update of the information

containing data related to known malware object in the server-side AV database (315);

the data processing module (313) being connected to the request processing module (311), the user profile database (312) and the forced update module (317), wherein the data processing module (313) is configured to generate requirements to dynamically update the user-side AV database (216) based on the parameter changes received from the user profile database (312) and the notification received from the forced update module (317); and by

a data selection module (314) configured to receive the requirements to update the user-side AV database (216) from the data processing module (313) and for preparing required data by selecting a subset of the data related to known malware objects from the server-side AV database (315),

wherein the server update module (316) is connected to the data selection module (314) and is further configured for sending the subset to the user computer (120-128, 210) for updating the user-side AV database (216); and

wherein the parameter changes comprise changes in the user geographical location."

Claim 1 of auxiliary request 1 differs from that of the main request in that the "server update module" is claimed as also being:

"... to support by the user-side AV module (211) to scan the user computer (120-128, 210) for malware objects; ..."

Claim 1 of auxiliary request 2 differs from that of the main request in that the phrase referring to the user

parameters now reads as follows (insertions underlined by the board):

"... wherein the user data comprises user parameters collected for registration that include a user ID, a user geographical location used by the system to form a country-dependent signature database, an AV application version, an AV database version, visited site statistics permitting determining types of threats that can appear after visiting particular sites, and which are used by the system to form the user-side AV database (216) and detected malware statistics used by the system to provide signatures corresponding to the most common malware objects; ..."

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 relates to antivirus (AV) databases which are explained to "contain various tapes of data" like "malware signatures [...], blacklists of malicious object checksums, blacklists of web sites, executable codes of data unpacking algorithms and codes of heuristic data analysis", but also, more generally, "data for dealing with detected threats" or other things ("etc.") (see page 1, lines 22-27). It notes that AV databases have to be frequently updated to maintain a required level of data security (see page 1, lines 22-27; page 2, lines 6-7; see also figure 1). Due to the size of the AV databases, this may be impractical.

1.1 It is explained that users will normally not need the "full AV database". For instance, if they "never visit" certain domains on the web, they will not need black-lists for that domain (page 4, lines 20-28). Or, depending on the OS version of a user, certain threats may be real or not (page 4, line 29, to page 5, line 4).

1.2 To reduce the amount of data to be transmitted, the application proposes the dynamic generation of a smaller AV database for each user, selected from the full AV database based on "user parameters". These include a user ID, the geographical user location, user computer information (e.g. the OS), visited site statistics and detected malware objects statistics (see page 5, line 30, to page 6, line 13), and they are uploaded as a "user profile" on initial registration of the user PC with the update server (see figure 1, no. 110). The created (smaller) user AV database is transmitted to the user PC (see page 5, lines 16-24, and page 7; figures 1 and 2, nos. 111 and 216).

1.3 Updates of the user-side AV database take place either at the user's request (see figure 3, no. 311; and page 8, paragraphs 1 and 3), when user-parameters have changed (see page 3, paragraph 2) or when signatures have been added to the server-side AV database (see figure 3, no. 317; and e.g. page 9, paragraph 3).

The prior art

2. D3 discloses a system in which a server assists a client, typically a mobile communication device, in determining whether an application (also referred to as a "data object", see paragraph 24) should be installed or remain so (see abstract).

2.1 The client transmits to the server the data object to be analysed and further data relating to the device - e.g. the device's OS or battery limitations (see paragraphs 27 and 30) - or the data object - e.g. "behavioral data" such as the likelihood the data object will "crash", or metadata (see paragraphs 31, 33-34 and 99).

2.2 The server assesses the data in view of several potential risks, e.g. that the data object is malware or spyware, contains coding flaws, or is a drain on battery power (see paragraphs 32, 78, 95, 126 and 128). The server returns a (binary or fuzzy) "assessment" (see paragraph 35, especially lines 14-17, and paragraph 99, last sentence).

2.3 The server may store the transmitted data, i.e. the data objects and the client data (see paragraph 36, lines 6-8; paragraph 46; figure 1, no. 111). If asked for an assessment, the server may return one delivered earlier without having to compute it anew, unless, obviously, the data object must be reassessed because it or the device data have changed in the meantime (see paragraph 37, e.g. lines 8-12; see also paragraphs 44, 48 and 105).

2.4 To reduce the necessary data transmissions, the client may keep assessments in a local cache (see paragraph 112). The server may also send unrequested assessments to the clients but, to save storage, only relating to data objects which the client might actually wish to install because they are compatible with its OS or the device's "country, language or area code" (see paragraph 117, in particular the last sentence). D3 also discloses that "devices will cache assessments for the data objects they are most likely

to encounter" , where this prediction may be made "based on [...] previous encounters" (see paragraph 119). It also suggests that the "optimal amount of assessment data to cache on a device may be different depending on user behavior" (see paragraph 120).

Clarity, Article 84 EPC, and claim construction

3. A central element of the claimed invention is the fact that certain "user parameters" are taken into account "for generating a user-side AV database", namely "a user ID, a user geographical location, an AV application version, an AV database version, visited site statistics and detected malware object statistics".

3.1 The alleged effect of these parameters is that they enable the generation of an "optimal AV database for individual users" in the sense that they "provide for maximum PC protection while having a minimal size" (see the application, page 6, lines 26-29).

3.2 Claim 1 according to the main request and auxiliary request 1 does not define how these parameters are used "for generating" the user-side AV database. Auxiliary request 2 attempts to address this issue for some of the parameters. In the following, the parameters are discussed individually.

3.3 The "user ID" is a unique number (see the description, page 5, last line) which identifies the user but is not, in itself, a "critical user parameter that" would "affect the content of the AV database" (see page 4, lines 18-19).

3.4 The "user geographical location" can be used, so the application (page 6, lines 1-2 and 14-15), "to form the signatures database", disclosed as a part of a typical AV database (see page 1, lines 22-27), which may be "country-dependent, or language dependent". The board understands this as saying that the user AV database will contain, depending on the user's geographical location, different malware signatures. Which ones these are is not disclosed. Therefore, it cannot be judged whether it is permissible to assume that, depending on geographical location, the risk of certain malware can be neglected, let alone how malware with negligible risk based on geographical location is determined.

3.5 The "AV application version" and "AV database version" are merely disclosed as possible user parameters (page 6, lines 6 and 7), but their relevance is not further explained. During oral proceedings, the appellant stated that, depending on the version number of AV application and database, different (types of) data (see page 1, lines 22-27) could be processed on the user-side. Accordingly, the skilled person would have understood, based on their common knowledge, that only content suitable for the "versions" in question are considered "for generating" the user-side AV database. However, the board considers that the application contains no indication that this is the correct interpretation.

3.6 The "visited site statistics" is disclosed as "permit[ting] determining the types of threats that can appear after visiting particular sites or categories of sites" (see page 6, lines 19-21). It appears to be intended (although it is not claimed) that the statistics relate to what the individual user may have

done as opposed to, for instance, all users. However, the application does not explain how sites a user may have visited are mapped to potential or actual (types of) threats and how the frequency of such visits is taken into account when deciding how to generate the AV database.

3.7 The "malware object statistics" is referred to as "detected malware object statistics" (see page 6, line 8), and it is disclosed that "the AV database receives only the signatures corresponding to the most common malware objects". It is not clear from the description whether the claimed malware statistics relate to individual users - i.e. the selection of malware objects on individual user sides - or all users, which would thus entail the selection of generally more common malware objects.

3.7.1 In the latter case, the "malware object statistics" is not user-specific. If, accordingly, the server-side AV database contained only "the signatures corresponding to the most common malware objects" in the first place, no selection would have to be made for the user-side AV database at all.

3.7.2 In the former case, it is not clear how user-specific malware statistics are meant to be produced and updated. When the AV application and database are first installed, no user-specific malware statistics can exist and thus be taken into account for generating the AV database. Moreover, it is not claimed that the user-side AV database may be updated (or how) when such user-specific statistics become available. Finally, the consideration of only "common malware objects" expresses, at best, a trade-off between security and AV database size. With regard to less common malware

objects, the user's computer will end up not being protected; i.e. "maximum user PC protection" is not achieved.

4. Due to the above shortcomings, claim 1 of all three requests is unclear insofar as it is not defined how the mentioned user parameters affect the generation of the user-side AV database, Article 84 EPC. Moreover, it cannot be established that - or under what conditions - the created user-side AV database actually provides "for maximum user PC protection while having a minimal size". The board is also not aware of - and the appellant did not contribute - any other specific effect which would have to be attributed to the use of the mentioned "user parameters" "for generating" the user-side AV database.

Inventive step, Article 56 EPC

5. D3 is a suitable starting point for assessing inventive step.

6. In comparing D3 with the invention as claimed, the board takes the following view.

6.1 The "assessments" produced according to D3 include, in a broad sense, "data related to known malware objects". When assessments are stored on the server or the client, they form, respectively, a server-side and user-side "AV database". Moreover, the assessments stored on the user side are a subset of those stored on the server and are selected in view of "user data", in particular, device information including the operating system, country or language (see D3, paragraphs 112, 117) or user data (see paragraphs 119 and 120).

6.2 D3 discloses that the user device information is stored on the server (see paragraph 46, lines 1-18). In the board's view, the totality of this information qualifies as a "user profile database" in the sense of the claims.

6.3 D3 discloses that "application data" and "device data" may change, that the assessments may therefore have to be reproduced, and that the new results will be stored on the server (i.e. "inserted into the user profile database") and transmitted to the clients (see paragraph 105). At least for some clients, this qualifies as a "forced update" in the sense of the claims.

6.4 D3 discloses some sort of user-side software contributing to the overall AV service (see paragraph 128) and thus a user-side "AV application" in a broad sense (see the main request and auxiliary request 2), but not a user-side AV module which would "scan the user computer for malware objects" (see auxiliary request 1, claim 1, line 15-16 and 19-20).

6.5 D3 also discloses that the user geographical location is taken into account to decide which assertions to transmit to the user device, i.e. which ones to use "for generating" the user-side AV database in the mentioned sense (see paragraph 117, last sentence).

6.6 D3 does not disclose the following features of the invention claimed in the main request:

(i) An initial registration of what happens at that point, and

(ii) that user parameters include a user ID, a (user-side) AV application version, a (user-side) AV database version, visited site statistics and detected malware object statistics.

6.6.1 As regards auxiliary request 2, D3 also does not disclose that the:

(ii') visited site statistics permit determining types of threats that appear after visiting particular sites, and which are used by the system to form the user-side AV database and that the malware object statistics are used by the system to provide signatures corresponding to the most common malware objects.

6.6.2 As regards auxiliary request 1, D3 does not disclose:

(iii) a user-side AV module which would "scan the user computer for malware objects" (see auxiliary request 1, claim 1, lines 15-16 and 19-20).

6.7 With reference to feature (i), the registration of user devices is at least a conventional - and thus obvious - measure. Likewise, it is obvious to send "device data" (see D3, paragraph 30) or other user data (see paragraph 117) to the server as early as possible and, more specifically, "upon initial registration" if registration were to take place.

6.8 Furthermore, with regard to features (ii) and (ii'), D3 discloses the transmission of only particularly relevant assessment data to the user device, in view of user location (see paragraph 117), user hardware, user behaviour or user preferences (paragraphs 119 and 120). This would have prompted the skilled person to consider further "user parameters" that affect which assessments

would be more relevant to transmit. At this general level, it would have been obvious for the skilled person to consider additional parameters such as the claimed ones. Furthermore, the particular choice of parameters cannot, in the board's judgment, contribute to inventive step because what effect their consideration has - or under what considerations - cannot be determined for the claimed subject-matter as a whole (see point 4 above).

6.9 Finally, with regard to feature (iii), the board considers it generally obvious as a matter of load balancing between the server and the user device to provide the user device with an "AV module" performing some of the antivirus scanning. Moreover, if this were the case, it would have been obvious for the user device to, for instance, not scan a "data object" for which an assessment happens to be available in the local cache. In this case, the cache, considered to be the user-side AV database within the meaning of claim 1, would "support [...] the user-side AV module [...] to scan the user computer [...] for malware objects".

7. Thus, claim 1 of none of the pending requests shows the required inventive step over D3, Article 56 EPC.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

L. Stridde W. Sekretaruk

Decision electronically authenticated