Internal distribution code:

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

Datasheet for the decision of 20 November 2018

Case Number: T 2535/16 - 3.5.06

Application Number: 13172224.1

Publication Number: 2750072

IPC: G06F21/57, G06F21/62

Language of the proceedings: EN

Title of invention:
System and method for protecting cloud services from unauthorized access and malware attacks

Applicant:
Kaspersky Lab, ZAO

Headword:
Trust level determination/KASPERSKY

Relevant legal provisions:
EPC Art. 56, 84

Keyword:
Inventive step - all requests (no)
Claims - clarity (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 2535/16 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 20 November 2018

Appellant: (Applicant)	Kaspersky Lab, ZAO 39A/3 Leningradskoe Shosse Moscow 125212 (RU)
Representative:	Sloboshanin, Sergej V. Füner, Ebbinghaus, Finck, Hano Mariahilfplatz 3 81541 München (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 14 June 2016 refusing European patent application No. 13172224.1 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 14 June 2016, refusing European patent application 13 172 224.1 for lack of inventive step over, *inter alia*, the documents

D1: US2008/005285 A1 and
D3: US 2007/124805 A1.

II. Notice of appeal was filed on 5 August 2016, the appeal fee being paid on the same day. A statement of grounds of appeal was received on 14 October 2016. The appellant requested that the decision be set aside and a patent be granted on the basis of claims according to a main or 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 over D1 and D3, Article 56 EPC. Clarity objections were also raised, Article 84 EPC.

IV. In response to the summons, with a letter dated 19 October 2018, the appellant filed amended sets of claims 1-14 according to a main and an auxiliary request. During the oral proceedings held on 20 November 2018, the appellant also filed an amended claim 1 according to an auxiliary request 2, with the other claims to be adapted if claim 1 were to be found allowable. The auxiliary request of 19 October 2018 will therefore be referred to as "auxiliary request 1" hereinafter.

V. Independent claims 1 and 7 of the main request read as follows:

"1. A method for processing queries from a user device (120) by a server (130), the method being performed by the server (130), and comprising:

receiving from an antivirus software (121) deployed on the user device (120), system state and configuration data that is automatically and periodically collected from the user device (12) and indicative of use of the user device (120);

receiving different queries based on the system state and configuration data collected by and automatically transmitted from the antivirus software (121) of the user device (120) directed to different cloud-based security services (140-190) provided by the server (130), wherein the server (130) requires a predefined procedure for contacting the different cloud-based security services, wherein the predefined procedure includes contacting the different cloud-based security services (140-190) in a specific order;

analyzing the system state and configuration data of the user device (120) to determine a level of trust associated with the user device (120);

analyzing the different queries received from the antivirus software (121) to determine whether the different queries are used to contact the different cloud-based security services (140-190) according to the specific order required by the predefined procedure;

based on the determination of whether the different queries are used to contact the different cloud-based security services (140-190) according to the specific order required by the predefined procedure, determining whether to update the level of trust associated with the user device (120); and

determining, based on the level of trust, how to process the different queries, wherein the determining step comprises rejecting the queries from the antivirus software (121) or processing the different queries by the different cloud-based services (140-190) and providing the processing results of the cloud-based security services (140-190) as response to the antivirus software (121).

7. A server (130) for processing queries from a user device (120), the server (130) being configured to:

receive from an antivirus software (121) deployed on the user device (120), system state and configuration data indicative of use of the user device (120);

receive different queries based on the system state and configuration data collected by and automatically transmitted from the antivirus software (121) of the user device (120) directed to different cloud-based security services (140-190) provided by the server (130), wherein the server (130) requires a predefined procedure for contacting the different cloud-based security services (140-190), wherein the predefined procedure includes contacting the different cloud-based security services (140-190) in a specific order;

analyze the system state and configuration data of the user device (120) to determine a level of trust associated with the user device (120);

characterized in that the hardware processor (15) is further configured to:

analyze the different queries received from the antivirus software (121) to determine whether the different queries are used to contact the different cloud-based security services (140-190) according to the specific order required by the predefined procedure;

based on the determination of whether the different queries are used to contact the different cloud-based security services (140-190) according to the specific order required by the predefined procedure, determine whether to update the level of trust associated with the user device (120); and

determine, based on the level of trust, how to process the different queries, wherein the determining comprises rejecting the queries from the antivirus software (121) or processing the different queries by the different cloud-based security services (140-190) and providing the processing results of the cloud-based security services (140-190) as response to the antivirus software (121)."

Claims 1 and 7 of auxiliary request 1 are identical to those of the main request, except that the following phrase was added to the step of "receiving" (resp. "receive"):

"... and wherein the different cloud-based security services (140-190) comprise at least two of a file reputation service (140), an Internet address reputation service (150), a statistics service (160), a whitelist service (170), an anti-spam service (180), and a software activation service (190);

Claim 1 of auxiliary request 2 corresponds to claim 1 of the main request, except that in its preamble the phrase "being performed by the server (130), and" was deleted, that the steps of "receiving", "analyzing", and "determining", two each, were qualified by the phrase "by the server (130)", and that the step of "receiving different queries" now reads as follows (additions are underlined, deletions struck through):

"... receiving, by the server (130) [,] different queries based on the system state and configuration data collected by and automatically transmitted from the antivirus software (121) of the user device (120) directed to different cloud-based security services (140-190) provided by the server (130), wherein the server (130) ~~requires~~ provides rules comprising a predefined procedure for contacting the different cloud-based security services to the user device (120), wherein the predefined procedure includes contacting the different cloud-based security services (140-190) in a specific order ..."

VI. 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 protecting cloud-based security services against unauthorized access and malware attacks (see page 3, lines 1-2).

1.1 The system considered in the application is depicted in figure 1a. Antivirus programs installed on user devices (see figure 1a, number 120) will "automatically and periodically collect" and send "information about malware detected on the user devices, unknown and/or suspicious objects [...] on the user devices [...], and other security related information" to a "cloud infrastructure" (see figure 1a, numbers 130 and 160, and page 6, paragraphs 1 and 2) which will, in turn, provide several "security services" to the clients (see page 6, paragraph 2).

1.2 These services include "reputation services" indicating whether individual files or internet addresses are found to be malicious or spam (file and internet address reputation services, anti-spam service) or whether individual objects are known to be safe (whitelist service), a "statistics service" collecting the data based on which of the corresponding "verdicts" are obtained, and a software activation service for license handling (*loc. cit.)*.

1.3 The quality of these security services depends on the trustworthiness of the user devices. An attacker might undermine it by having a large number of user devices send false information to the cloud service so that it will incorrectly confirm a piece of malware to be safe (see page 2, last paragraph).

1.4 In order to protect the reputation-based cloud service against malware attacks, a "validation module" is provided (figure 1b, number 133) which maintains a "level of trust" for each user device. Only two specific levels of trust are disclosed: "trusted" and "untrusted" (see e.g. page 9, last paragraph; page 10, paragraph 2; page 11, lines 20 to 24).

1.5 The determination of the level of trust depends on the "system configuration" or "the location of the user device" and "the accuracy of the procedure used by the user device", e.g. whether the device is used "for its intended purpose" and follows the "accurate procedure" when interacting with the cloud service, e.g. by "contact[ing] the cloud services in [the correct] sequence" (see paragraph bridging pages 8 and 9; page 10, paragraphs 2 and 3; page 15, paragraph 2, to

page 16, paragraph 3; page 17, paragraph 3, to page 18, paragraph 3; and figure 1b, numbers 134-136).

1.5.1 A "query processing module" (figure 1b, number 131) will check the current level of trust of a user device to decide whether to pass information from that device to the cloud services (page 9, paragraph 2) and whether to respond to a query from that device (paragraph 3).

1.6 The (licensed) antivirus programs store the "rules which specify the right procedure for contacting cloud services" (page 15, lines 16-17) so that they know what is expected from them to earn trust. It is disclosed that these rules may change periodically and may be sent to the licensed antivirus software [..] together with other updates (see page 17, lines 7-9).

Claim construction and clarity, Article 84 EPC

2. Claim 7 specifies a server configured to perform several steps, including one of "receiv[ing] from an antivirus software [...] deployed on the user device [...] system state and configuration data", as well as "different queries". With the user device not being part of the server, steps carried out on the user device can only be limiting on claim 7 if and insofar as the server can determine these steps from the received data. More specifically, it is not limiting on the server whether (or how often) the transmitted data is "collected" on the user device or that it is antivirus software to collect the data.

2.1 The same applies to claim 1, directed towards a "method for processing queries from a user device [...] by a server". Claim 1 of the main request and auxiliary request 1 explicitly require "the method[to be]

performed by the server". Claim 1 of auxiliary request 2 no longer contains that phrase, but explicitly specifies only the steps to be carried out "by the server". Accordingly, it is unclear whether the fact that an antivirus software runs on the user device and "automatically and periodically collect[s]" certain data specifies steps of the claimed method.

2.2 In view of the foregoing, the presence of user device features in claims directed towards the server alone is considered to render them unclear, Article 84 EPC.

2.3 However, for the purposes of the analysis below and to the appellant's benefit, the board interprets claims 1 and 7 as specifying, respectively, a method to be carried out on the server and a user device, and a system comprising the server and at least one user device.

3. The security services are not defined in the main request or auxiliary request 2. Claim 1 of auxiliary request 1 states that there are "at least two" of them, options being identified by name but otherwise remaining unspecified. It is not precisely defined in the claim what a "statistics service" or a "software activation service" is meant to do or what makes all the claimed services "security" services. Both claims also leave open whether - and, if so, how - the security services relate to, depend on or interact with each other.

4. The independent claims of the main request and auxiliary request 1 remain vague about the role of the "specific order required by the" server. In the board's view, they allow two different interpretations.

4.1 According to the first one, the "specific order" constitutes a kind of secret which the server shares with the security software and/or its user, and which the latter has to use much like a password or a PIN to get access to certain services.

4.2 According to the second one, the "specific order" describes assumptions on how trustworthy software is conventionally assumed to behave.

4.3 In the first scenario, the specific order may be essentially arbitrary and, moreover, its function will be independent of whether it relates to contacts with "security services" or to other types of actions. On the other hand, the specific order will have to be communicated to the licensed antivirus software.

4.4 In the second scenario, the specific order need not be communicated to the user device. On the other hand, it is more plausible to assume that well-behaved antivirus software follows a specific order for reasons relating to the nature of the services. For instance, a whitelist service can quickly identify a suspicious file as safe, while a reputation service might require more time for its decision. Hence, it appears reasonable to assume that a well-behaved antivirus service would, for efficiency reasons, contact the whitelist service before the reputation service. In contrast, a malicious antivirus software wanting to manipulate the reputation service might not contact the whitelist service at all.

4.5 In the board's view, this ambiguity has significant implications for the claimed system and methods and, indeed, on the comparison of the claimed invention with

the prior art (in particular the claimed "specific order" and the "staged cookies" of D3; see below).

4.6 The board considers that the unclear nature and role of the claimed "specific order" render claims 1 and 7 of the main request and auxiliary request 1 unclear.

4.7 Claim 1 of auxiliary request 2 makes it clear that the intention was for claim 1 to specify scenario 1, which is originally disclosed on page 17, lines 7-9 (see also the appellant's letter of 19 October 2018, page 4, point 2.3).

The prior art

5. D1 relates to network admission control (NAC), i.e. making sure that "only endpoint devices" complying with a desired security policy" and thus being "trusted" "[may] connect to other devices in the network" (see paragraph 2). A client's policy compliance is assessed based on the client's "configuration" or "posture", e.g. whether certain software is installed and up-to-date, based on features like "status, usage or resource capacity" of certain processes running on the device, or other "settings" (paragraphs 6, 36, and 40). The assessment is in dialog between a policy server and a piece of local software called a "policy key" (figure 2, paragraphs 41-43). Network access may be restricted or entirely prohibited for non-compliant devices or users (see, for instance, paragraphs 35, 48 and 53). If non-compliance is determined, the user may be directed to a "remediation service", which may, for instance, inform the user by means of a webpage about the software to be downloaded or installed to (re-)establish compliance (see paragraph 34).

6. D3 relates to the use of "staged cookies" to control users' access to specific network services without them having to log in in the conventional way (see paragraphs 1 and 3). The basic idea is that users must be "associated with" a required level of trust before they can access a certain "special" network service (see e.g. paragraphs 12 and 21, and figure 4). Users can earn trust by exhibiting certain behaviour, in particular by "valid interactions" with the server (see e.g. paragraphs 26 and 33), or lose trust by showing unexpected behaviour, such as not selecting at least one link returned by a search service (see paragraph 32). If a client shows such expected behaviour, it may be concluded that "a true user is operating the client, and the client is not simply programmed to perform tasks intended to circumvent the authorization module" (*loc. cit.*). If a valid action is completed as expected, a staged cookie is issued. When a user requests a particular service, its trust level is determined based on the staged cookies the user has acquired until then, and the service request is granted if a "trust threshold" is exceeded (paragraphs 28 and 34). It is also disclosed that the presence of a "sequence of staged cookies" may be used as a trust criterion (paragraph 34).

Inventive step

Auxiliary request 2

7. The board agrees with the examining division that D1 is a suitable starting point for assessing inventive step of the claimed invention.

7.1 The appellant argued that "D1 [was] not a close prior art for the claimed invention", as was apparent from the fact that the examining division had "already acknowledged patentability of claim 1" in its communication "of February 11, 2015 and changed its opinion later on" (see grounds of appeal, page 3, paragraph 3).

7.2 The board disagrees with this position, noting that this preliminary opinion of the examining division is, firstly, preliminary and, secondly, has no bearing on whether D1 is a suitable starting point for the assessment of inventive step.

7.3 The appellant did not provide other reasons why the inventive-step assessment of the claimed invention should not start from D1.

8. The examining division found (see the decision, page 4, paragraphs 3 and 4; page 4, penultimate paragraph to page 5, paragraph 1; and point 1.2, items a) and b)) that the then claim 1 differed from D1 in that

a) the "queries" of D1, i.e. the network access requests, came from the "user devices" rather than from the local "security software", i.e. the "policy key", and
b) the level of trust associated with the user devices was not disclosed in D1 as being determined based on whether the security software on the user device has "contact[ed] the different security services according to a specific", "predefined order".

8.1 The appellant took the view that D1 also did not disclose the server to

c) "receiv[e] different queries from the security software of the user directed to different security services", in particular "cloud-based services" (see the grounds of appeal, page 5, paragraph 2, and the letter of 19 October 2018, page 3, paragraph 2).

8.2 With the claim interpretation as chosen above (see point 3.3), the board agrees that differences a)-c) exist. More specifically, in view of the amended claim 1 of auxiliary request 2, the board considers the following:

a/c) D1 does not disclose that antivirus software on the client computer accesses "security services", but only that certain "endpoint devices" access "other devices within the network" (see e.g. paragraph 2).

b) D1 does not disclose that trust is determined based on a "specific order" in which accesses have to be made and which is provided by the (policy) server to the endpoint devices.

8.3 With regard to difference a/c), the board notes that queries from a user device will always come from (or at least via) some sort of software - for instance, interface software operated by a user - and other devices within the network will always have to be contacted for a purpose which, broadly speaking, may be considered a service. The board also considers that the term "cloud-based" is unsuitable for distinguishing the claimed system architecture from the network access of D1.

8.4 Difference a/c) thus boils down to the fact that the claimed invention requires the queries to be from and to particular kinds of software: "antivirus software"

and "security services". It thus has the effect of making the access control of D1 available to a different - if vaguely described - application scenario.

8.5 Difference b) has the effect of providing an additional mechanism for establishing trust in the endpoint devices of D1.

8.6 As explained above (points 4.1 and 4.3), the board is of the opinion that the requirement of a "specific order" of accesses must be construed as independent of the nature of the software accessing or being accessed. As a consequence, the inventive step of both differences may be assessed separately.

8.7 Further concerning difference a/c), the board takes the view that it is obvious that the network discussed in D1 may run a known cloud-based reputation service such as that mentioned in the application (see page 2, lines 1-2).

8.8 As regards difference b), the board considers that the skilled person, setting out to improve the trust determination of D1, would come across D3. This assumption *per se* was not challenged by the appellant.

8.8.1 The appellant argued that D3 did not "teach or suggest a predefined sequence of services that are to be contacted" as a trust criterion "but only [...] a predefined sequence of staged cookies" (see the grounds of appeal, page 7, paragraph 1, last sentence, and paragraph 3; page 8, paragraph 1, last sentence). In its letter of 19 October 2018 (page 6, point 3.6), it further stated that detecting a "predefined sequence of staged cookies" on a client system had to "mean that the user performed the specific actions" associated

with the individual staged cookies " in the set 'predefined sequence'" but did not imply that the required sequence of staged cookies was "actually known by software of the user device".

8.8.2 The board understands D3 as disclosing that individual "staged cookies" are issued to clients after having "completed" the actions relating to a "normal service request" (see paragraphs 32-33 and figure 3, in particular nos. 110, 112, 114 and 116). In that sense, the "sequence of staged cookies" disclosed as a trust criterion (paragraph 34) represents a sequence of completed "normal service requests". D3 does not put any particular stress on which requests these might be. Moreover, as discussed above, the board considers it to be immaterial for feature b) that the sequence is one of queries to cloud service-based security services.

8.8.3 It is true that D3 leaves open whether the sequence of staged cookies mentioned in paragraph 34 is one agreed between server and clients or one representing an expected sequence of actions. Notably, the example of paragraph 32 does not imply the second interpretation, as the expected action (click a result after requesting an Internet search) completes a single (normal) service request and leads to the issuance of only one staged cookie (see again paragraphs 32 and 33).

8.8.4 D3 discloses in paragraph 34 that the access to a special service request may be based on the number of staged cookies in the "cookie jar" or some kind of point system, which, in turn, may be based on the type of request, other associated user actions or, "on other criteria" such as "a predefined sequence of staged cookies, or other system".

8.8.5 This language invites the skilled reader to consider variations and modifications of the explicitly disclosed point systems. On that basis, the board considers it obvious for the skilled person to implement the requirement of a "predetermined sequence of cookies" as one provided by the server to the clients.

8.9 Accordingly, the board comes to the conclusion that neither difference a/c) nor difference b) establishes an inventive step of claim 1 of auxiliary request 2 over D1, Article 56 EPC.

Main request

9. Claim 1 of auxiliary request 2 being a clarification and limitation of claim 1 of the main request results in the preceding argument regarding the former applying directly to the latter. Therefore, claim 1 of the main request also lacks inventive step, Article 56 EPC.

Auxiliary request 1

10. The reference to some specific security services which are, however, only referred by name and not further defined, does not affect the above assessment. In particular, it does not change the board's finding under point 8.6 above that the kind of services and the trust criterion "specific order" do not interact with each other so that differences a/c) and b) can be assessed separately, nor that under point 7 that the network of D1 might run security services as claimed. The board therefore concludes that claim 1 of auxiliary request 1 also lacks inventive step, 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