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 June 2017

Case Number: T 1179/14 - 3.5.06

Application Number: 12164389.4

Publication Number: 2515252

IPC: G06F21/00

Language of the proceedings: EN

Title of invention:
System and method for reducing security risk in computer network

Applicant:
Kaspersky Lab, ZAO

Headword:
Reducing security risk/KASPERSKY

Relevant legal provisions:
EPC Art. 56

Keyword:
Inventive step - (no)

Decisions cited:

Catchword:

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 1179/14 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 20 June 2017

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 24 January 2014 refusing European patent application No. 12164389.4 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 lies against the decision of the examining division, with reasons dispatched on 24 January 2014, to refuse European patent application No. 12 164 389.4 for lack of inventive step over document

D1: US 2010/125911 A1.

II. Notice of appeal was filed on 21 March 2014, the appeal fee being paid on the same day. A statement of grounds of appeal was filed on 9 May 2014. The appellant requested that the decision under appeal be set aside, and that a patent be granted on the basis of the claims according to a main or an auxiliary request as filed with the grounds of appeal, the other application documents being:

description pages
3-17 as originally filed, and
1, 2, 2a received on 14 November 2012, and
drawing sheets
1/8-8/8 as originally filed.

III. In an annex to a summons to oral proceedings, the board informed the appellant of its preliminary opinion that, *inter alia*, the independent claims of both requests lacked inventive step over D1.

IV. In response to the summons, by letter of 19 May 2017, the appellant filed amended claims 1 to 12 according to a main and an auxiliary request.

V. Oral proceedings were held on 20 June 2017. During them, the appellant filed an amended method claim 1 labelled "auxiliary request 2" and explained that

independent system claim 7 would be amended accordingly once claim 1 had been discussed.

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

"A computer-implemented method for reducing security risk in a computer network, the method comprising:

collecting from a plurality of computers in the network information about computer usage, security incidents, and electronic communications between computer users;

retrieving, for each computer user, a user profile comprising at least a personal and professional information of the user, and a plurality of risk factors associated with the user;

calculating, for each computer user, values for the plurality of risk factors in the user profile based on the computer usage information collected from the computer of each user;

calculating, for each computer user, a user security rating based on the values of one or more risk factors of the plurality of risk factors in the user profile;

automatically adjusting a security rating of at least one computer user based on (i) the personal or professional information of said at least one computer user, and communication flow events comprising usage of single data storage media by the at least one computer user,

characterized in that

security rating of at least one computer user is further based on (ii) communication flow events comprising data transmissions within the computer network by the at least one computer user, and messaging between the at least one computer user and at least one other computer user within the computer network, and social communications comprising a

probability of electronic communication flow between the at least one computer user and the at least one other computer user, and the security rating of the at least one other computer user; wherein

security settings for the plurality of computers are automatically selected based on the security ratings of the users of said computers; and

the selected security setting is applied to respective protection agents executing in the plurality of computers to reduce security risk in the computer network."

VII. Claim 1 of the first auxiliary request has the same preamble as claim 1 of the main request, its characterising portion reading as follows:

"... security rating of at least one computer user is further based on (ii) communication flow events comprising data transmissions within the computer network by the at least one computer user, and messaging between the at least one computer user and at least one other computer user within the computer network, and social communications comprising a probability of electronic communication flow between the at least one computer user and the at least one other computer user, and the security rating of the at least one other computer user, and (iii) external drive usage events; wherein

security settings for the plurality of computers are automatically selected based on the security ratings of the users of said computers, wherein different security settings include different network security settings based on determined traffic limitation levels and prohibitions on launching of executable files from external drives, wherein the traffic limitation levels are based on a plurality of website browsing levels for

each of the respective plurality of computers; and wherein the selected security setting is applied to respective protection agents executing in the plurality of computers to reduce security risk in the computer network, wherein the network security settings are based on the determined traffic limitation level and are applied to the respective protection agent that enables a corresponding traffic check on the respective computer."

VIII. Claim 1 of auxiliary request 2 is identical to claim 1 of the first auxiliary request except that, in the final "wherein" clause, the redundant phrase "are based on the determined traffic limitation level and" has been deleted and the following passage added at the end:

"... and wherein the prohibitions setting are applied to the respective protection agent to enable prohibition of launching of executable files from external drives."

IX. At the end of the oral proceedings, the chairman announced the board's decision.

Reasons for the Decision

The invention

1. The application is concerned with reducing the security risks in a computer network based on individual users' security ratings.

1.1 The security ratings are calculated based on the users' personal characteristics and their behaviour, including

their use of external drives, the Internet and social media, the frequency with which they install software and how many security incidents they have had (see page 5, last paragraph; page 6, paragraph 3, to page 7, paragraph 2; page 8, paragraph 4, to page 9, paragraph 2; table 1 on pages 12-13; page 14, lines 4-17; figures 2-4 and 6). Moreover, the users' communication behaviour is monitored, and an individual user's security rating takes into account both communication with another user that takes place and that which is merely "probable" in view of the proximity of the two users' locations or the similarity of their job duties (see page 8, paragraphs 2-3, and figure 2, "detection agent" 210 and "event log" 220).

1.2 Based on the security ratings, "security settings" are selected for each individual user and sent to a "protection agent" on the user's computer (see figure 2, nos. 230 and 240). The protection agent may be (a component of) an "antivirus application, responsible for spam filtering, spoofing, detection of network attacks and viruses" (see page 7, lines 21-25) or a "firewall" (see page 15, table 2 and lines 3-5). The "selected security settings" may include "settable parameters for various components of the protection agent" and relate to "security policies of the computers, software usage and installation restrictions, network access settings, computer usage restrictions, user training materials, and administrative notifications" (see page 7, lines 23 and 26-28, and page 11, lines 1-4).

1.3 More specifically, it is disclosed that the system according to the invention may prohibit a user from launching executable files from external drives if that user has been using "many external drives", or impose

"traffic limitations" such as "traffic checks" or the "disabl[ing of] the access to unauthorized web sites" depending on the user's "website browsing level" (see page 7, last paragraph, to page 8, paragraph 1; page 14, lines 4-17; and figure 15, table 2). Alternatively, the administrator may order "preventive measures" such as training programs or "other sanctions" (see page 11, last eight lines, and figure 7).

The prior art

2. D1 discloses a system that continuously tracks each user's activities so as to produce a "risk score" (abstract, paragraphs 33, 38, 40, 47, figures 1 and 7-9) and to assess the user's compliance with a given security policy (see paragraphs 15 and 16).

2.1 If the user does not comply with the security policy, an administrator may be alerted (see paragraph 15, last sentence). If the user's risk score is too high, various protective measures may be taken, including training and mentoring of the user, improving business processes or "modify[ing] the security policies enforced on the users" (see paragraph 16, fourth and last sentences, and paragraph 47, last two sentences).

2.2 Various user activities are tracked, including web browsing, the use of email and of hardware peripherals, and the activity in the computer's file system (see figure 7, no. 701a-d, paragraph 68). Moreover, entire sequences of user activities are detected and evaluated, such as the downloading and launching of executable code from a web browser, the copying of files from USB sticks, and the installation of software (see figures 9c and 9d, e.g. sequences 5, 7 and 11). By

way of example, it is mentioned that emails are dangerous in particular if the "recipient[s]" are "outside the organisation" (see paragraphs 73 and 74, and figure 7, no. 701b, dash 4).

Inventive step

Main request

3. D1 discloses the features of the preamble of claim 1, namely the collection of "information about computer usage, security incidents and electronic communications between computer users" (see esp. D1, figure 7), the retrieval of "user profiles" (see e.g. paragraph 33), the calculation of a "user security rating" (see e.g. abstract) and the use of that rating so as to "reduc[e] security risk[s]" in a computer network.

3.1 D1 further discloses that a user's security rating is determined based *inter alia* on "communication flow events comprising data transmissions" (see figure 7, no. 701a and b) and that email conversation with users outside the organisation is riskier than with users within it (see paragraphs 73 and 74).

3.2 D1 does not, however, disclose the following features of claim 1:

(a) A user's security rating is based on messaging or "social communication" between the user and *a specific* other user, on the "probability of electronic communication flow" between users, or on the security ratings of the user's communication partners.

(b) There are "protection agents" on the users' computers which receive the determined "security settings" and use them "to reduce security risk in the computer network".

4. *Re difference (b)* D1 discloses the generation of a detailed risk report for each individual user for assessment by the system administrator (see figures 11a-k, paragraph 86). On the basis of this report the system administrator decides on any consequences (see paragraphs 16 and 47). To enforce them, D1 discloses training, mentoring or the threat of dismissal (paragraph 47).

4.1 The board considers it to be obvious that a system administrator may also want to address undesirable behaviour with individual prohibitions: for example, if a user performs particularly risky operations such as visiting unauthorised websites or accessing a private USB stick from his office computer, an obvious sanction would be to prohibit such operations for that user.

4.2 The decision to impose a sanction is, in the board's judgement, a non-technical decision by the system administrator.

4.3 Claim 1 of the main request does not specify what the protection agent does and thus how precisely it contributes to enforcing the security settings. The description includes the option of sending training material or administrative notifications to the user concerned (see page 11, paragraph 1). From that perspective, the claimed protection agent may be construed as merely providing automated support for the sanction disclosed in D1.

4.4 The board takes the view that such automation *per se* is obvious and thus cannot give rise to an inventive step.

5. *Re difference (a)* The fact that, according to difference (a), further security-related parameters are considered may improve risk assessment and thus help the system administrator to address security risks.

5.1 The board agrees with the decision under appeal (see reasons 7.4) that the idea of adjusting a user's security rating in view of the security rating of that user's communication partners is an administrative decision which thus cannot, *per se*, contribute to an inventive step.

5.2 Moreover, the board takes the view that the idea is obvious over D1. D1 already discloses that email communication with users outside the organisation is riskier than with users within it. It is merely a small modification of this idea to treat individual users separately. Furthermore, the board considers it to be well known that some websites are more likely to cause malware infections than others. Accordingly, it would be obvious to treat some websites as riskier than others. The same consideration applies by analogy to a user's different communication partners.

5.3 If determining a security rating requires establishing the security ratings of users with which a given user communicates or might communicate (see the application, page 8, lines 8-18), it would be straightforward for the person skilled in the art to provide means for obtaining them.

6. The board concludes that differences (a) and (b) are insufficient to render the subject-matter of claim 1 inventive over D1.

Auxiliary requests 1 and 2

7. Claim 1 of the first auxiliary request adds the features that

(c) the users' security ratings are also based on "external drive usage events",
(d) the security settings may comprise prohibitions on launching executable files,
(e) depending on a user's "website browsing levels", corresponding "traffic limitation levels" are determined, and
(f) the protection agents may "enable" corresponding "traffic checks".

Claim 1 of auxiliary request 2 clarifies that the security settings according to (b) are "applied" to the protection agent and that it is the role of the protection agent to "enable" prohibition of launching executable files from external drives.

7.1 D1 discloses the detection of external drive usage events and of users' "website browsing levels", as well as their use for determining security ratings (see e.g. figure 7, no. 701d).

7.2 The board considers it obvious that a system administrator will, when detecting that an individual user performs activities considered to be particularly risky, consider checking these activities more carefully or prohibiting them entirely. For instance, the board considers it obvious to require that a user

stop using "external drives" or visiting specific websites. Where possible, it would also be obvious, in the board's judgement, to use automated support, e.g. in the form of a "protection agent" on the user's computer, to enforce such prohibitions.

7.3 As a consequence, the board also finds the subject-matter of claim 1 of auxiliary request 2 to lack inventive step over D1, Article 56 EPC. *A fortiori*, this argument also applies to claim 1 of the first auxiliary request.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated