Internal distribution code:

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

Datasheet for the decision of 10 January 2017

Case Number: T 1243/11 - 3.5.06

Application Number: 06300970.8

Publication Number: 1768043

IPC: G06F21/00, H04L29/06

Language of the proceedings: EN

Title of invention:
Information system service-level security risk analysis

Applicant:
ALCATEL LUCENT

Headword:
Service-level security risk analysis/ALCATEL LUCENT

Relevant legal provisions:
EPC 1973 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 1243/11 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 10 January 2017

Appellant: (Applicant)	ALCATEL LUCENT 148/152 route de la Reine 92100 Boulogne-Billancourt (FR)
Representative:	Hirsch & Associés 137, rue de l'Université 75007 Paris (FR)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 3 March 2011 refusing European patent application No. 06300970.8 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 3 March 2011, to refuse European patent application No. 06 300 970.8 for lack of inventive step over the document

D7: US 6 883 101 B1.

II. Notice of appeal was filed on 12 May 2011, the appeal fee being paid on the same day. Also on 12 May 2011, a statement of grounds of appeal was filed. The appellant requested that the decision be set aside and that a patent be granted based on claims 1-20 according to the main request or one of two auxiliary requests as filed with the grounds of appeal, in combination with the application documents as originally filed.

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

"An apparatus comprising:

a risk analyzer (76) configured to identify one or more assets of an information system that have respective relationships with a service provided by the information system, and to determine one or more security risks to the service by analyzing effects of security vulnerabilities which are associated with the identified assets and are propagated to the service through the relationships; and

an interface (52) operatively coupled to the risk analyzer and configured to provide a consolidated representation (154, 184) of the service, the consolidated representation comprising an indication (174, 206) of the one or more determined security risks

and an indication (175, 177, 202, 224, 226) of at least one of the respective relationships between the service and the one or more identified assets, the indication (174, 206) of the one or more determined security risks comprising, for each determined security risk, respective indications (232, 233, 234, 235, 236, 237, 238, 239) of an overall security state associated with the security risk and a plurality of security sub-states comprising the overall security state."

In claim 1 of the first auxiliary request, the specification of the "consolidated representation" was amended to read as follows (additions to claim 1 of the main request underlined):

"... consolidated representation comprising respective icons representing at least one or more identified assets, an indication (174, 206) of the one or more determined security risks and an indication (175, 177, 202, 224, 226) of at least one of the respective relationships between the service and the one or more identified assets, ..."

In claim 1 of the second auxiliary requests, the specification of the "consolidated representation" was further amended to read as follows (additions to claim 1 of the main request underlined):

"... consolidated representation comprising respective icons representing at least one or more identified assets, an indication (174, 206) of the one or more determined security risks associated to each respective icon and an indication (175, 177, 202, 224, 226) of at least one of the respective relationships between the service and the one or more identified assets, ..."

Moreover, at the end of claim 1 of the second auxiliary request, the following phrase has been added:

"... the indication of at least one of the respective relationships specifying the type of relationships among a plurality of types."

Each of the requests also contains an independent method claim 15 corresponding closely to apparatus claim 1, and a machine-readable medium claim 20 defined by reference to the method claims.

IV. In an annex to the summons to oral proceedings, the board informed the appellant of its preliminary opinion that the subject-matter of claim 1 lacked inventive step, Article 56 EPC 1973, for the reasons given in the decision under appeal.

V. In response to the summons, the appellant did not file either amendments or arguments. Instead, with letter dated 14 November 2016, it withdrew its request for oral proceedings and informed the board that it would not be attending the scheduled oral proceedings.

VI. With letter dated 16 December 2016, the oral proceedings were then cancelled. The following reasons are based on the board's preliminary opinion as communicated to the appellant.

Reasons for the Decision

The invention

1. The application is concerned with "service-level security risk analysis" of a networked system and

automated support for administrators to make "operational decisions" based on the determined vulnerabilities. More specifically, as an aspect of "proactive security", it is central for network operators to "understand the security state [...] at any given time and to assign a priority action list for risk mitigation" (see page 2, paragraph 2).

1.1 It is disclosed that in "common Network Management Systems (NMSs)" the "view of a managed communication network is limited to physical topology of interconnected systems" and lacks information on "higher layers [relating to] service, business, or functional priorities" (page 2, paragraph 3).

1.2 It is further disclosed that there were "management systems available" which provided "some sort of service-level view" in graphical form as a chart of a hierarchical graph (see page 3, paragraph 1 *et seq.*). Even these systems, however, presented only a "limited or incomplete view of service-level status or security risks", especially related to its related assets (page 3, paragraph 2).

1.3 The claims relate to an information system comprising "physical and logical assets" and a service "provided by the information system" which is "defined by relationships between" assets of both kinds. Figure 6 lists various hardware and software components as possible assets (see also page 28, paragraph 2).

1.4 The invention according to claim 1 of all requests relates to a "risk analyser" and an "interface", the risk analyser "configured to identify one or more assets of an information system" related to a service "provided by the information system" and "to determine

one or more security risks by analysing security vulnerabilities associated with the identified assets", the interface providing suitable "representations" and "indications".

The prior art

2. The description discloses as the starting point for the present invention a number of systems supporting the system administrator in assessing the security of a given system. In particular, "common Network Management Systems" provide views of the "physical topology of interconnected systems" and other "management tools" go beyond that in providing a "service-level view" using a graphical user interface. The board understands the description as acknowledging such systems as being prior art in the sense of Article 54(2) EPC 1973.

3. D7 discloses a system that performs risk analysis of a network in terms of its nodes and displays it to the administrator to assess and act upon (see e.g. Figures 7, 8b, 10). D7 does not display a "service-level view" in addition to the "network topology". Therefore, D7 can roughly be summarized as a system which corresponds, as regards the displayed content, to the "common Network Management Systems" mentioned on page 2 of the description and, as regards the graphical user interface, to the "management tools" on page 3.

The decision under appeal

4. The decision found that claim 1 of the main request differed from D7 in that particular security risks were "indicated" (i.e. displayed) in a particular way (see decision, page 4, last paragraph). This was considered to solve the objective technical problem of adapting

the system of D7 "to meet a security-administrative requirement to allow security administrator[s] to do more informed risk assessment and mitigation decisions" (page 5, lines 1-5). The required information was stated to constitute a "requirements specification for the task assigned to" the security administrator (page 5, entire paragraph 1) and it was found obvious for the skilled person to adapt the system of D7 accordingly (reasons 12.2, page 5, penultimate paragraph). Substantially the same argument was made with respect to the auxiliary request (page 7, paragraphs 1 and 2, and reasons 13.1).

The appeal

5. The appellant argued in particular why D7 neither disclosed nor suggested the determination and display of risk information regarding the execution of a specific service on a specific device (see the grounds of appeal, page 3, lines 16-20) and that the specific details of the interface claimed allowed the user to see certain bits of information "at a glance" (see pages 4 and 6, penultimate paragraphs).

6. However, the appellant does not address, let alone challenge, the opinion of the examining division that, in a nutshell, the claims are concerned with determining and displaying what, according to some externally given, "administrative" requirement, needs determining and displaying.

Claim construction

7. Claim 1 of all requests refers *inter alia* to

- an "information system comprising physical and logical assets",
- a "service being defined by relationships between [...] physical and [...] logical assets",
- "one or more assets of a selected service" being "identified",
- "security vulnerabilities" being "associated with the identified assets", and
- the security vulnerabilities being "propagated to the service through the relationships".

7.1 The board notes that neither the "information system" nor the "service", "assets" or "vulnerabilities" are defined any further, but takes the view that this terminology, albeit very broad, is sufficiently clear to allow an assessment of inventive step.

7.2 Specifically, the board considers that claim 1 makes reference to a system comprising several "assets", some of which are used by a "service" running on the system, and that there are (or may be) "vulnerabilities" which relate to individual assets on the system and thus, indirectly, to the service relying on them.

Inventive step

8. Such systems were known in the art, as was the knowledge about vulnerabilities that might affect it. The description confirms this (see pages 3 and 4), and the appellant did not challenge the corresponding statement made by the board in the annex to the summons to oral proceedings.

8.1 From this perspective, the board agrees with the decision under appeal that the claimed invention addresses the problem of providing the administrator

with information that is required to assess the security of a given type of information system in view of certain predetermined vulnerabilities.

8.2 More specifically, the technical problem to be solved over such a system can be considered to be the implementation of a suitable interface for presenting the administrator with relevant bits of information in an intelligible form.

8.3 This statement of the technical problem is consistent with the description which states as a disadvantage of prior art systems that they provide only limited or incomplete information (see pages 3 and 4, *inter alia* page 3, lines 17-19).

8.4 That the information that needs to be displayed is "identified", "selected" and "determined" (see claim 1 of the main request referring to "identified assets", a "selected service" and "determined security risks") is an immediate consequence of the problem to be solved. *How* this is done is neither claimed nor, as it seems, described.

8.5 The board considers that it would be obvious for the skilled person to adapt the known prior art systems as specified above to display the desired information.

8.6 In the board's view, this applies also to the provision of the specifically claimed interface features, in particular of

(a) an "indication [...] of the [...] determined security risks and [...] for each [of them] of an overall security state [...]", and an "indication [...] of the [...] respective relationships between

the service and the [...] identified assets" as claim 1 of the main request requires, of

(b) "icons representing [the] identified assets" with associated risks, as claim 1 of the first auxiliary request additionally requires, and of

(c) an "indication [...] of the [...] respective relationships specifying the type of relationships" as claim 1 of the second auxiliary request additionally requires.

8.7 In this regard, the board also notes that these interface features are, apart from being obvious, exclusively concerned with presenting information to the user (who can thus see certain information "at a glance", see point 5 above) and therefore make contributions exclusively in a field excluded from patentability, see Article 52(2)(d) EPC.

8.8 As a consequence, the apparatus according to claim 1 of all three requests lacks inventive step over the prior art systems mentioned in the application, Article 56 EPC 1973.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated