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 12 December 2017

Case Number: T 2018/13 - 3.5.03

Application Number: 04724272.2

Publication Number: 1730917

IPC: H04L29/06

Language of the proceedings: EN

Title of invention:
Method and system for network intrusion detection, related network and computer program product

Applicant:
III Holdings 1, LLC

Headword:
Method and system for network intrusion detection/III Holdings

Relevant legal provisions:
EPC Art. 56
RPBA Art. 12(2), 12(4)

Keyword:
Inventive step - main request and first auxiliary request (no)
Admissibility - second auxiliary request (no)

This datasheet is not part of the Decision.
It can be changed at any time and without notice.

Decisions cited:
G 0007/93, T 0573/09, T 0556/13

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

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 2018/13 - 3.5.03

DECISION
# of Technical Board of Appeal 3.5.03
of 12 December 2017

Appellant:
(Applicant)

III Holdings 1, LLC
2711 Centerville Road, Suite 400
Wilmington, DE 19808 (US)

Representative:

Carpmaels & Ransford LLP
One Southampton Row
London WC1B 5HA (GB)

Decision under appeal:

Decision of the Examining Division of the European Patent Office posted on 3 May 2013 refusing European patent application No. 04724272.2 pursuant to Article 97(2) EPC

Composition of the Board:

Chairman F. van der Voort
Members: K. Schenkel
O. Loizou

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division refusing European patent application No. 04724272.2, international publication number WO 2005/099214 A1.

II. The refusal was based *inter alia* on the ground that the subject-matter of claim 1 of the main request did not involve an inventive step (Article 56 EPC) having regard to the disclosure of:

D3: FREDERICK K.K.: "Network Intrusion Detection Signatures, Part 5", [online], 16 April 2002, pages 1-4

and the common general knowledge of a person skilled in the art.

In its decision and in two communications, the examining division also referred to:

D4: ZHANG Y. ET AL.: "Detecting Backdoors", [online], 2000, pages 1-11.

The first and second auxiliary requests were not admitted into the proceedings because, due to various features having been deleted from claim 1, they were considered to relate to a different subject than the main request. Further, claim 1 of both requests lacked clarity (Article 84 EPC), claim 1 of the late-filed second auxiliary request contravened Article 123(2) EPC, and the subject-matter of claim 1 of both requests did not, *prima facie*, involve an inventive step (Article 56 EPC).

III. In its statement of grounds of appeal, the appellant requested that the decision be set aside and that a patent be granted on the basis of the claims of a main request or, in the alternative, of one of first and second auxiliary requests, all requests as filed with the statement of grounds of appeal.

The appellant also conditionally requested oral proceedings.

IV. In a communication following a summons to oral proceedings, the board, without prejudice to its final decision, raised objections under Articles 84 and 123(2) EPC against claims 1, 8 and 16 of the main request and the first auxiliary request as well as objections under Article 52(1) EPC in conjunction with Article 56 EPC in respect of the subject-matter of those claims, starting out from:

D1: NORTON M. ET AL.: "The new Snort", COMPUTER SECURITY JOURNAL, COMPUTER SECURITY INSTITUTE USA, vol. 19, No. 3, 2003, pages 37-47, ISSN: 0277-0865.

With respect to the second auxiliary request, the board indicated that its admissibility and, if admitted, the question of inventive step for the subject-matter of claim 1 needed to be discussed at the oral proceedings. Further, claims 1, 5 and 10 did not appear to comply with Article 123(2) EPC.

V. Oral proceedings were held on 12 December 2017.

The appellant's final requests were that the decision under appeal be set aside and that a patent be granted on the basis of the claims of the main request or, in the alternative, of one of the first and second auxiliary requests, all requests as filed with its statement of grounds of appeal.

At the end of the oral proceedings, after due deliberation, the chairman announced the board's decision.

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

"A method of providing network intrusion detection (6) in a network (2) wherein data flows are exchanged using associated network ports and application layer protocols, the method including the step of monitoring (14) data flows in said network (2), characterised by further comprising the steps of:

- maintaining in a repository a plurality of application layer protocol identification signature sets, each set corresponding to an application layer protocol independently of any predefined association between said network ports and said application layer protocols;
- maintaining in a repository a plurality of misuse detection signature sets (68), each set corresponding to an identified application layer protocol and being indicative of possible misuse occurring in the communications with the identified application layer protocol independently of any predefined association between said network ports and said application layer protocols;
- identifying (16) the application layer protocols involved in said monitored data flows, by matching (22) a current data flow against an application layer protocol identification signature set for identifying at least one application layer protocol involved in said current data flow;

- responsive to the identification, selecting one of the plurality of misuse detection signature sets (68) corresponding to said identified application layer protocol;
- providing intrusion detection (18) on said monitored data flows by matching the current data flow against said selected misuse detection signature set (68); and
- responsive to a misuse being detected (70), by generating a security event (38)."

VII. Claim 1 of the first auxiliary request differs from claim 1 of the main request in that, in the second and third paragraphs, the wording

"maintaining in a repository"

has been replaced by

"storing in a memory".

VIII. Claim 1 of the second auxiliary request reads as follows:

"A method of providing intrusion detection (6) in a network (2) wherein data flows are exchanged using associated network ports and application layer protocols, the method including the step of monitoring (14) data flows in said network (2), characterised by further comprising the steps of:

- maintaining an integrated signature set integrating a protocol identification signature set (24) and a misuse detection signature set (68);
- establishing a network policy (34) including a plurality of conditions which must be satisfied by data flows;

- performing (22) a set-wise matching of a current data flow against the integrated signature set, for identifying at least one application layer protocol involved in said current data flow and for detecting a misuse (70) in said current data flow for an identified application layer protocol independently of any predefined association between said network ports and said application layer protocols;

- comparing (32) the identified application layer protocol with said network policy; and

- responsive to a misuse being detected, either in said step of performing (22) a set-wise matching or in said step of comparing (32), generating (38) a security event."

IX. Claim 1 of the first auxiliary request as decided on by the examining division reads as follows:

"A method of providing intrusion detection (6) in a network (2) wherein data flows are exchanged using associated network ports and application layer protocols, the method including the step of monitoring (14) data flows in said network (2), characterised by further comprising the steps of:

- providing an integrated signature set integrating a protocol identification signature set (24) and a misuse detection signature set (68);

- establishing a network policy (34);

- performing (22) a set-wise matching of a current data flow against the integrated signature set, for identifying at least one application layer protocol involved in said current data flow and for detecting a misuse (70) in said current data flow for an identified application layer protocol independently of any predefined association between said network ports and said application layer protocols;

- comparing (32) the identified application layer protocol with said network policy (34); and

if a misuse is detected, either in said step of performing (22) a set-wise matching or in said step of comparing (32), generating (38) a security event."

Reasons for the Decision

1. *Main request - claim 1 - inventive step*

1.1 The closest prior art is considered to be represented by D1, which is also concerned with the detection of network intrusion (see page 37, second paragraph, "The Protocol Flow Analyzer classifies network application protocols into client and server flows. In-depth analysis of these protocol data flows allows Snort to make intelligent decisions ...", the header on each page "ATTACKS AND COUNTERMEASURES", and the footer on each page "Computer Security Journal" (underlining added by the board)).

The method employs rules which are matched against the data (page 37, first paragraph, "The multi-pattern search engine uses a two-stage architecture to inspect data and find rule matches."). In order to enhance the processing speed, the method of D1 uses rule optimisation which includes the creation and selection of rule sets in order to inspect only one rule set against each packet (page 40, right-hand column, section "Rule Optimization"). The board considers that these rule sets correspond to the misuse detection signature sets referred to in claim 1. It further goes without saying that there has to be a repository to maintain the created rule sets.

D1 further discloses the use of associated network ports (page 39, right-hand column, paragraph "Rule Optimizer", "Since these subsets are based on the unique rule parameters such as source port, destination port and rule content ...") and protocols, whereby the method includes the step of monitoring data flows in the network (page 37, first paragraph). The generation of alarms in response to the detection of a misuse or, in other words, security events is disclosed implicitly ("Together, these enhancements greatly improve the performance and efficiency of Snort and help reduce false alarms", ibid.).

The rule sets are created on the basis of rule parameters which are different for each transport protocol (page 40, section "Rule Set Creation", "The rule optimizer creates these rule sets during initialization by using the most unique Snort rule parameters. The chosen rule parameters are different for each transport protocol, because each transport protocol has different parameters that make them unique. For instance, a TCP rule may be unique from other TCP rules based on the source and destination ports, while an ICMP rule may be unique based on the ICMP type of that rule. The rule optimizer takes all of these unique parameters and forms rule subsets based on them. This gives the multi-rule detection engine much smaller rule sets to inspect." (underlining added by the board)). Hence, each rule set corresponds to only one transport protocol.

For each packet that is processed, a rule set is selected (page 40, last full sentence). Selection is also based on the rule parameters (page 41, first paragraph, "It is important to note that the rule optimizer is the first stage of the multi-rule search engine, because the selection of the rule set depends on matching some of the packet parameters to the rule parameters.", and page 43, section "Rule Set Selection", "Once Snort proceeds to the rule-processing stage for each packet, the packet parameters are passed to the rule manager to select the appropriate subset of rules to apply to a packet. Once the rule set is selected, the multi-rule search processing begins."). Because each rule set, or in other words subset of rules, corresponds to one transport protocol, the selection of a rule set includes the identification of the corresponding transport protocol. This is also supported by an example given for the IP protocol (page 41, right-hand column, last paragraph, "The rule optimizer supports the IP protocol by using the IP transport protocol field. All IP rules that include TCP, UDP or ICMP are grouped into that particular protocol rule set" and "In practice, the rule optimizer uses the transport protocol information to create and select efficient rule sets").

1.2 The appellant argued that D1 repeatedly referred to network ports and disclosed rule sets based on network ports (see, for example, page 37, first paragraph, "The first stage of the multi-pattern search engine is a high-speed set-based inspection engine, which quickly identifies potential rule matches based on content and ports").

The board notes however that D1 discloses four categories of rule sets, only one of which, namely the category "Packet anomaly rules", is based on network ports, see pages 44 and 45, section "Rule Sets and Search Types". The other three are independent of network ports. Hence, D1 also discloses rule sets which are not based on network ports and therefore are independent of any association between network ports and protocols.

1.3 D1 therefore discloses, using the language of claim 1,

a method of providing network intrusion detection in a network wherein data flows are exchanged using associated network ports and transport protocols, the method including the steps of

- monitoring data flows in said network,
- maintaining in a repository a plurality of misuse detection signature sets, each set corresponding to an identified transport protocol and being indicative of possible misuse occurring in the communications with the identified transport protocol independently of any predefined association between said network ports and said transport protocols;
- identifying the transport protocols involved in said monitored data flows;
- responsive to the identification, selecting one of the plurality of misuse detection signature sets corresponding to said identified transport protocol;
- providing intrusion detection on said monitored data flows by matching the current data flow against said selected misuse detection signature set; and
- responsive to a misuse being detected, by generating a security event.

1.4 The method of claim 1 thus differs from the method of D1 in that it uses the application layer protocol instead of or in addition to the transport protocol, in that the application layer protocols involved in said monitored data flows are identified by matching a current data flow against an application layer protocol identification signature set, and in that it further comprises the step of maintaining in a repository a plurality of application layer protocol identification signature sets, each set corresponding to an application layer protocol independently of any predefined association between said network ports and said application layer protocols.

1.5 A technical effect of further taking into account an application layer protocol as a parameter in the method of D1 when forming rule sets is that their size can be further reduced. In this respect, the board notes that D1 already discloses smallest possible rule sets as a requirement for the rule optimiser (page 40, right-hand column, paragraph "Rule Set Creation", point 1, "Create the smallest, most efficient rule sets possible.").

With respect to protocol identification by means of signature analysis, the board notes that D1 discloses that the selection of the rule set depends on matching some of the packet parameters to the rule parameters, but does not give details of this matching.

1.6 Starting out from D1, the technical problem underlying the subject-matter of claim 1 may thus be seen in further reducing the size of the rule sets and in providing an implementation of rule set selection.

1.7 With respect to using the application layer protocol for creating rule sets, the board notes that D1 itself already suggests taking the application layer protocols into account (page 40, left-hand column, first paragraph, "For example, if Snort is run with 1,500 rules, these rules get divided into smaller subsets based on transport and application-layer protocols." (underlining added by the board)).

Further, the skilled person, starting out from D1 and faced with the second part of the above-mentioned technical problem, would consider document D4, since it is also concerned with the detection of misuse in a network (see title and abstract).

More specifically, D4, page 5, discloses at the beginning of section 4 "Special-Purpose Detection Algorithms" the use of signature analysis for detecting the protocol used ("In this section we explore algorithms that look for signatures reflecting the use of particular protocols"). The use of a repository for maintaining these signatures is implicit.

The skilled person faced with the above-mentioned problem would therefore follow the suggestion given in D1 by adding the application layer protocol as a further parameter and by using the signature analysis of D4 to detect the application layer protocol. He would thus arrive, without exercising inventive skill, at a method of providing network intrusion detection which includes all the features of claim 1.

1.8 The appellant, in its statement of grounds of appeal, argued that D4 already disclosed an intrusion detection system and, hence, that the skilled person would not combine it with another intrusion detection system. The monitoring according to D4 simply checked whether the expected protocol was used on a predetermined port, and the detection of an unexpected protocol would be the final result which did not need any further monitoring or processing.

The board, however, is not convinced by these arguments. The method of D4 includes the steps of first identifying the protocol and then checking whether it is used on the standard port for this protocol (page 5, section 4 "Special-Purpose Detection Algorithm", first paragraph, "In this section we explore algorithms that look for signatures reflecting the use of particular protocols. If we then find servers for those protocols running on ports other than their standard ones, such instances may indicate the presence of a backdoor."). The step of identifying protocols by means of signatures is thus not inextricably linked to the step of checking whether the identified protocol is used on the standard port and can therefore be used independently for the sole purpose of identifying protocols in another intrusion detection method, such as the one in D1.

1.9 For the above reasons, the board concludes that the subject-matter of claim 1 of the main request does not involve an inventive step (Articles 52(1) and 56 EPC).

2. First auxiliary request - claim 1 - inventive step

The only difference between the subject-matter of claim 1 of the main request and that of claim 1 of the first auxiliary request is that the signature sets are not maintained in a repository but stored in a memory.

In the technical field of data processing, to which the subject-matter of claim 1 relates, any means for holding data, such as a signature set, may be designated as a memory. Therefore the feature does not further limit the claimed subject-matter.

For this reason and the reasons set out in point 1 above, the board concludes that the subject-matter of claim 1 of the first auxiliary request does not involve an inventive step (Articles 52(1) and 56 EPC).

3. *Second auxiliary request - admissibility*

3.1 Claim 1 of the second auxiliary request (see point VIII above) differs from claim 1 of the first auxiliary request as decided on by the examining division (see point IX above) in that in the second auxiliary request

(a) in the second paragraph the claim reads "maintaining an integrated signature set" instead of "providing an integrated signature set";

(b) in the third paragraph, instead of "establishing a network policy (34)", it reads "establishing a network policy (34) including a plurality of conditions which must be satisfied by data flows"; and,

(c) in the last paragraph, instead of "if a misuse is detected", it reads "responsive to a misuse being detected".

3.2 Differences (a) and (c) are of a linguistic nature, whilst difference (b) does not add any limitation to the subject-matter, since a network policy implicitly includes conditions which are to be satisfied. Thus claim 1 of the second auxiliary request and claim 1 of the first auxiliary request as decided on by the examining division have essentially the same subject-matter. This has not been contested by the appellant.

The examining division did not admit the first auxiliary request into the proceedings under Rule 137(3) EPC, stating *inter alia* (see Statement of reasons, point 2) the following:

"The feature "selecting a misuse detection signature set corresponding to said identified application layer protocol" present in claim 1 of the main request was removed from claim 1 of both auxiliary requests and is thus not present in claim 1 of both auxiliary requests. Furthermore, also the feature "identifying the application layer protocols ... independently of any predefined association between said network ports and said application layer protocols" present in claim 1 of the main request was removed in claim 1 of both auxiliary requests and is thus not present in both auxiliary requests, claim 1 of both auxiliary request [sic] merely define that "detecting a misuse in said current data flow for an identified application layer protocol independently of any predefined association between said network ports and said application layer" and thus the independency of any predefined association between said network ports and said application layer in claim 1 of both auxiliary requests refers to detecting the misuse but not to identifying at least one application [sic] application layer protocol. The Applicant has thus changed the subject to be protected, by removing previously introduced feature(s) relating to a subject and adding other feature(s) relating to a different subject. Particularly, the auxiliary requests are directed to another subject than the main request, see also T2096/09.";

"Moreover, the features "an integrated signature set integrating a protocol identification signature set and a misuse detection signature set" and "set-wise matching ... against the integrated signature set" in claim 1 of both auxiliary requests are the

[sic] vague und unclear, Article 84 EPC, and it is unclear which further technical features are associated with these features."; and

"Notwithstanding the clarity objection above, the newly introduced features in claim 1 of both auxiliary requests concerning the integrated signature set and its set-wise matching are prima facie not inventive, Article 56 EPC.".

3.3 The board refers to G 7/93 (OJ EPO 1994, 775), according to which "if an Examining Division has exercised its discretion under Rule 86(3) EPC [1973 (now Rule 137(3) EPC)] against an applicant in a particular case and the applicant files an appeal against the way in which such discretion was exercised, it is not the function of a Board of Appeal to review all the facts and circumstances of the case as if it were in the place of the first instance department, in order to decide whether or not it would have exercised such discretion in the same way as the first instance department. If a first instance department is required under the EPC to exercise its discretion in certain circumstances, such a department should have a certain degree of freedom when exercising that discretion, without interference from the Boards of Appeal. In the circumstances of a case such as that before the referring Board, a Board of Appeal should only overrule the way in which a first instance department has exercised its discretion if it comes to the conclusion either that the first instance department in its decision has not exercised its discretion in accordance with the right principles as set out in paragraph 2.5 above, or that it has exercised its discretion in an unreasonable way, and has thus exceeded the proper limits of its discretion." (Reasons 2.6).

3.4 Article 12(2) RPBA stipulates: "The statement of grounds of appeal and the reply shall contain a party's complete case. They shall set out clearly and concisely the reasons why it is requested that the decision under appeal be reversed, amended or upheld, and should specify expressly all the facts, arguments and evidence relied on.".

In the present case, as already pointed out in the board's communication following the summons to oral proceedings, the appellant did not give any reason in its statement of grounds of appeal why the board should set aside the examining division's discretionary decision under Rule 137(3) EPC not to admit the then first auxiliary request, which corresponds to the present second auxiliary request.

During the oral proceedings, the appellant argued, with reference to the examining division's finding that claim 1 of the second auxiliary request related to a different subject, that its subject-matter was not divergent. The board notes however that the examining division based its decision not to admit the first auxiliary request also on lack of clarity and a *prima facie* lack of inventive step. However, the appellant did not comment on these points.

Following T 573/09 (Reasons 2), since it was neither immediately apparent to the board upon reading the decision under appeal and the statement of grounds of appeal nor argued by the appellant at any point that the examining division had exercised its discretion in an unreasonable way or based it on the wrong principles, the board saw no reason to overrule the way in which the examining division had exercised its discretion.

3.5 The board also points to its own power under Article 12(4) RPBA to hold inadmissible requests which were not admitted in the first-instance proceedings and to the fact that the provisions of Rule 137(3) EPC also apply in appeal proceedings.

Exercising its own discretion under Article 12(4) RPBA (cf. T 556/13, Reasons 2.1.5 to 2.1.7), the board saw no reason not to hold the second auxiliary request inadmissible.

3.6 The second auxiliary request is therefore not admitted into the proceedings.

4. Conclusion

As there is no allowable request, it follows that the appeal is to be dismissed.

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

G. Rauh F. van der Voort

Decision electronically authenticated