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 July 2015

Case Number: T 2188/10 - 3.5.02

Application Number: 04755524.8

Publication Number: 1678692

IPC: G08B1/08

Language of the proceedings: EN

Title of invention:
System and Method for Monitoring and Detecting a Security Threat

Applicant:
Infraegis, Inc.

Relevant legal provisions:
EPC Art. 54(2), 84

Keyword:
Novelty - main request (no)
Claims - clarity - auxiliary request (no)

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 2188/10 - 3.5.02

D E C I S I O N
of Technical Board of Appeal 3.5.02
of 20 July 2015

Appellant: (Applicant)	Infraegis, Inc. 304 East Fairview Street, Suite 302 Arlington Heights, IL 60005 (US)
Representative:	inCompass IP Europe Limited 4 Bloomsbury Place London WC1A 2QA (GB)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 15 June 2010 refusing European patent application No. 04755524.8 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	R. Lord
Members:	H. Bronold
	W. Ungler

Summary of Facts and Submissions

I. The appeal concerns the decision of the Examining Division of the European Patent Office posted on 15 June 2010 refusing European patent application No. 04755524.8 pursuant to Article 97(2) EPC.

II. In a communication under Article 15(1) RPBA the board informed the appellant that it had concerns whether the subject-matter of the main request was novel.

III. Oral proceedings before the board were held on 20 July 2015.

IV. The appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of the claims of the main request filed with letter of 24 May 2010 or, if that was not possible, on the basis of the claims of the auxiliary request filed during the oral proceedings of 20 July 2015.

V. Reference will be made in this decision to the following document cited before the examining division:

D1: US 5,917,433 A.

VI. Claim 1 of the main request reads:

"A security system for providing a security service for monitoring a security status of at least one of a mobile asset and a fixed asset globally to detect and respond to a security threat, comprising:
an agent connected with a corresponding one of the at least one of the mobile asset and the fixed asset, said agent comprising:

multiple sensing devices for monitoring respective conditions relating to physical security and environmental security of the at least one of the mobile asset and the fixed asset;
a processor for compiling data relating to physical security and the environmental security to generate said security status including environmental and physical data; and
a transceiver for transmitting a data to and receiving data from the agent;
a computer system in communication with said agent for receiving said security status of said at least one of the mobile asset and the fixed asset;
a database for storing the received security status;
a threat detection analysis software for analyzing the security status to detect the security threat;
means configured to perform a process for determining a response to the detected security threat based on a type of security threat detected;
means for generating an output for performing the response in accordance with the process."

Independent method claim 9 claims a corresponding method for providing a security service.

VII. Independent claim 1 of the auxiliary request differs from claim 1 of the main request in that it is directed to multiple mobile assets and to multiple agents, and in that the feature dealing with communication of the agents was modified by introducing the following features at the end of the claim:

"a master control unit in communication with at least one of the agents for collecting the security status and retransmitting the security status to the computer system,

a position guidance system and a receiver for receiving a position data, and
the agents are in communication with other agents within range via a virtual intranet and with the master control unit for sending the security status and the position data to the computer system."

Independent method claim 8 is based on independent method claim 9 of the main request and comprises corresponding amendments.

VIII. The appellant essentially argued as follows:

Main request

Document D1 did not disclose a processor for compiling data relating to physical security and environmental security to generate said security status including environmental and physical data, a computer system for receiving said security status and a threat detection analysis software for analysing the security status. D1 merely made reference to sensing the temperature in a container and to sensing whether a container door is open. Nowhere did D1 discuss a security threat, the establishment of a security status or a threat detection analysis software.

Independent claim 1 was therefore novel over the disclosure of document D1.

Auxiliary request

The expression "virtual intranet" in the auxiliary request was clear since a skilled person was aware of the fact that a virtual network could be formed within an existing physical network, and would therefore have

understood that it specified the formation of ad hoc networks as and when agents came within range of each other.

Claim 1 of the auxiliary request was therefore clear.

Reasons for the Decision

1. The appeal is admissible

2. Main request - Article 54 EPC

2.1 Document D1 discloses a method and system of asset monitoring which determines the status of a shipping container. To this end, document D1 describes providing asset monitors 14 that can include multiple sensors 22 for sensing, for example, the temperature inside the container and whether the door of the container is open or closed (see column 6, line 62 to column 7, line 17).

Therefore, D1 discloses (see figure 1) an agent in the sense of claim 1 (the asset monitor 14) which is connected to at least one asset (the container 16 in which the asset monitor installed).

The agent according to D1 further comprises multiple sensing devices for monitoring the container and a processor for compiling data relating to physical and environmental security to generate said security status (see figure 2, sensors A and B and sensor interface 20, as well as column 13, lines 1 to 4, "the asset monitor 14 ... can monitor the sensors, via the sensor interface 20", and line 26 to 28, "...the asset monitor can be configured such that the sensed data is immediately transmitted to the central station...").

The agent according to D1 is also provided with a transceiver (see figure 2, reference 30).

The system of D1 further comprises a computer system in communication with said agent and a database (see figure 2, references 40, 42 and 46).

While document D1 does not literally disclose "conditions relating to physical security and environmental security", "physical and environmental data" or a "security status", it does nonetheless disclose features that directly and unambiguously fall within the meaning of these expressions in claim 1. Thus the temperature sensed by the temperature sensor constitutes environmental security data and the position of the door sensed by the door position sensor of D1 constitutes physical security data. Document D1 also discloses in column 13, lines 27 and 28 that "...the sensed data is immediately transmitted to the central station...". The sensed data according to D1 can therefore be regarded as a compiled "security status" which is transmitted to the computer system in the sense of claim 1.

Moreover, D1 discloses a threat detection analysis software (see column 7, line 49 to 54, "Based on this type of sensory signal, the ... central station ... can monitor the sensed condition, such as to detect trends or to determine if the sensed condition is within acceptable limits..."). Since the central station comprises a controller 42 connected to a memory 46, it is implicit that the central station is controlled by software.

The central station of D1 also represents means configured to perform a process for determining a response to the detected security threat, since according to column 11, lines 30 to 32, "...corrective action which is recommended to cure or alleviate the unacceptable condition..." is determined by the central station.

Furthermore, the central station of D1 represents means for generating an output for performing the response (see column 11, lines 28 to 31, "The central station can then respond, ..., with a message which details the corrective action...").

2.2 The appellant's counter-argument that D1 did not disclose that the asset monitor included a processor running software for carrying out the functions defined in the claim is not found convincing, because figure 2 of D1 shows that the asset monitor includes a "controller", which the skilled person would understand as implying a processor running appropriate software. Furthermore, as indicated above, the mere fact that D1 does not use the same terminology as the claim ("physical and environmental security", "security status" etc.) does not mean that such features are not disclosed in that document.

2.3 Thus, all features of claim 1 are known from the disclosure of document D1. The subject-matter of claim 1 of the main request is therefore not new in the sense of Article 54(2) EPC.

3. Auxiliary request - Article 84 EPC

3.1 The meaning of the expression "virtual intranet" inserted in claim 1 of the auxiliary request is not

clear in the context of the claimed system. The only basis for the amendment can be found on page 7, line 29 of the originally filed description, which passage does not enable it to be clarified.

The adjective "virtual" in relation to computer networks conventionally defines a network which is implemented using methods of network virtualisation, i.e. the "virtual" network is formed from network elements which are part of one or more physical networks, and which behave as if they were a single network, the virtual network, despite not being dedicated to that virtual network.

In contrast, the description of the application indicates that the mobile agents communicate with each other over a "virtual intranet" when they are "within range". The condition that communication among agents over the "virtual intranet" is in existence when the agents are within range does not imply any virtualisation of the network. The "virtual intranet" according to the description is therefore not virtual in the conventional sense, but is instead temporal, i.e. the intranet according to the description is created on an ad-hoc basis. The use of the adjective "virtual" in the description is thus in contradiction with its conventional meaning in the technical field of communication networks. Thus, the expression "virtual intranet" is not clear. Moreover, since the description does not contain a definition of the expression "virtual intranet", the skilled person can not deduce what is to be understood by a "virtual intranet" within the meaning of the original disclosure. Hence, no resolution of this contradiction would be possible within the constraints of Article 123(2) EPC.

3.2 Consequently, the auxiliary request does not meet the requirements of Article 84 EPC.

4. Since neither of the appellant's requests is allowable, the appeal has to be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

U. Bultmann R. Lord

Decision electronically authenticated