Method and system for alert classification in a computer network

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 October 2010 (07.10.2010)

PCT

(10) International Publication Number
WO 2010/114363 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04L 12/24* (2006.01)

(21) International Application Number:
PCT/NL2010/000060

(22) International Filing Date:
31 March 2010 (31.03.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/165,565 1 April 2009 (01.04.2009) US
2002694 1 April 2009 (01.04.2009) NL

(71) Applicant *(for all designated States except US)*: **UNIVERSITEIT TWENTE** [NL/NL]; 5, Drienerlolaan, NL-7522 NB Enschede (NL).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **BOLZONI, Damiano** [IT/NL]; 93, Mirastraat, NL-7521 ZG Enschede (NL). **ETALLE, Sandro** [IT/NL]; 7, Vijverlaan, NL-5042 PX Tilburg (NL).

(74) Agent: **SEITZ, H., F., K.**; Exter Polak & Charlouis B.V., P.O. Box 3241, NL-2280 GE Rijswijk (NL).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: METHOD AND SYSTEM FOR ALERT CLASSIFICATION IN A COMPUTER NETWORK

(57) Abstract: A method and a system for classification of intrusion alerts in computer network is provided. The method comprises the steps of monitoring traffic data in a computer network, detecting an intrusion, providing an intrusion alert and data in relation to the intrusion alert, generating a statistical analysis of the data in relation to the intrusion alert and classifying the intrusion alert based on said statistical analysis. The intrusion alerts and the data in relation to an intrusion alert may be generated by anomaly-based intrusion detection system. The generating a statistical analysis may comprise generating information about a statistical distribution of n-grams in the data. The classification may comprise comparing the statistical analysis with a model analysis of intrusion alerts with predefined alert classes. This model may be generated by providing a training set of data in relation to alerts, generating a model statistical analysis of said data, predefining at least two alert classes, and assigning predefined alert classes to the statistical analysis, based on information provided by a signature-based intrusion detection system, or by a human operator.

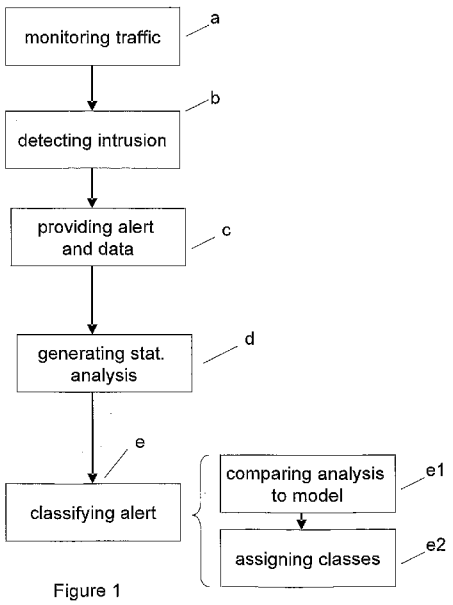

Figure 1

WO 2010/114363 A1

P29820NL00/MSM

Title: Method and system for alert classification in a computer network

Field of the invention

The present invention relates to a method and a system for classifying intrusion alerts in a computer network.

Background of the invention

Network intrusion detection systems (NIDS) are considered an effective defence against network-based attacks directed at computer systems and are employed in almost all large-scale IT infrastructures, due to the increasing severity and likelihood of such attacks. There are two main types of intrusion detection systems: signature-based and anomaly-based intrusion detection systems.

A signature-based intrusion detection systems (SBS) relies on pattern-matching techniques. The system contains a database of signatures, i.e. sequences of data, that are known from attacks of the past. These signatures are matched against the analyzed data. When a match is found, an alarm is raised. The database of signatures needs to be updated by experts after a new attack has been identified.

Differently, an anomaly-based intrusion detection systems (ABS) first build a statistical model describing the normal network traffic. The system then analyses data and flags any traffic or action that significantly deviates from the model, as an attack. The advantage of an anomaly-based system is that it can detect zero-day attacks, i.e. attacks that not yet have been identified as such by experts.

An SBS can detect not only when there is an attack, but can also classify the attack and provide information about the attack, since this information is usually provided in the database. An attack classification may identify the attack context with respect to the vulnerability exploited and the target. Typical examples of attack classifications are: buffer overflow, SQL Injection, Cross-site Scripting, path traversal, port scan and service fingerprinting.

These high-level classifications are often used by security teams to choose an appropriate counter measure policy or action, since attacks of a certain attack class may be more harmful than others. For instance, if a buffer overflow class alert is raised, the policy may be that the system will immediately deny any further communication to a certain IP, while in case of a port scan class alert, the system may wait for further action to take place.

An ABS generates and provides an attack alert when the currently analysed traffic data is too different from the model of normal traffic. Security teams have to manually inspect each alert

raised by the ABS to choose an appropriate counter measure policy or action, which results in a workload for the security team members. Several systems have been proposed to lower the workload for the security team members when alerts are raised by an ABS.

The US patent application US2007/0118905 describes a method for automatically classifying a set of alarms on the basis of specific trellis of the alerts. The specific trellis are merged into general trellis. Collated alerts are identified by selecting the alerts that are simultaneously the most pertinent and the most general. The collated alerts are supplied to an output unit of an alert management system.

In an article by W. Robertson et al., "Using generalisation and characterization techniques in the anomaly-based detection of web attacks" (conference proceeding NDSS symposium 2006), an anomaly based detection system of web-based attacks is disclosed. The system uses an anomaly generalization technique that automatically translates suspicious web requests into anomaly signatures. These signatures are then used to group recurrent or similar anomalous requests so that an administrator can easily deal with a large number of similar alerts. The grouping of signatures is done using ad hoc heuristics.

Summary of the invention

An objective of the present invention is to provide an other method and system for classification of intrusion alerts. This objective is achieved by providing a method for classifying intrusion alerts in a computer network, comprising the steps of monitoring traffic data in a computer network, detecting an occurrence of an intrusion from the monitored traffic data, providing in response to the detection of the occurrence of the intrusion, an intrusion alert and data in relation to the intrusion alert, generating a statistical analysis of the data in relation to the intrusion alert, and classifying the intrusion alert based on said statistical analysis.

An advantage of classifying intrusion alerts based on statistical analysis of the data in relation to the intrusion alerts may be that it provides a reliable method for classifying alerts which can be automated. Members of a security team need not to review all alerts and can choose an appropriate counter measure policy based on the classification. It may also enable that the policy is applied automatically on the basis of the classification.

In another embodiment, the second step of the method comprises detecting an anomaly on a basis of said monitoring and a model describing normal traffic data in a computer network.

An advantage of generating an intrusion alert when an anomaly has been detected may be that it doesn't require that the intrusion has to be identified once before for generating an intrusion alert. A yet unknown intrusion will also be detected when its activities result in deviation of the normal network traffic.

In a further embodiment of the invention, the data in relation to an intrusion alert comprises at least one payload of the traffic data that caused the intrusion alert. When an anomaly-based intrusion detection system raises an alert, the provided data may be a copy of the traffic data that has been identified as significantly deviating from a model that represents normal traffic data. The data in relation to the alert may also comprise other data collected or provided by the anomaly-based intrusion detection system.

In a further embodiment of the invention, generating a statistical analysis of the data in relation to the intrusion alert comprises generating information about a statistical distribution of n-grams in at least a part of the data in relation to the intrusion alert. An n-gram analysis is a sequence of n-units, with n being an integer. The unit can be a byte, a bit or another sequence of characters. In an embodiment of the invention the n-grams are sequences of bytes. In a further embodiment the information is about whether a certain n-gram has occurred in the data or/and the frequency of the occurrences. An advantage of generating this information may be that it provides an accurate profile of the data in relation to the alert and that it can easily be generated and compared with a model.

In an embodiment of the invention generating a the statistical analysis of the data in relation to the intrusion alert comprises applying a bloom filter on the statistical distribution of n-grams or storing the statistical distribution of n-grams in bitmap data structures. An advantage of applying a bloom filter or storing information in bitmap data structures may be that it enables efficient storage.

In another embodiment of the invention, classifying the intrusion alert comprises comparing at least a part of the statistical analysis with at least a part of a model of intrusion alerts with predefined alert classes and assigning one of the predefined alert classes to the intrusion alert based on the comparison. In a further embodiment, the model of intrusion alerts with predefined alert classes is generated before detecting an occurrence of an intrusion. An advantage of using a model for classifying the alerts may be that it enables automatic comparison of alerts generated by the ABS and known alerts, which have already been classified.

In another embodiment of the invention, generating a model of intrusion alerts with predefined alert classes comprises the steps of providing a training set of data in relation to intrusion alerts, generating a statistical analysis of said training set of data, predefining at least two alert classes, and assigning predefined alert classes to one or more parts of said statistical analysis, based on information provided by a signature-based intrusion detection system, or by a human operator and constructing a model of intrusion alerts comprising one or more parts of said statistical analysis and hereto assigned predefined alert classes. The training set may also comprise the traffic data with the known intrusion attacks. The data in relation to the alerts may then be generated by an ABS.

An advantage of this method of generating a model may be that it enables automatic generation of the model with only providing a training set and a appropriate classification.

In a further embodiment of the invention, the step of comparing at least a part of the statistical analysis with at least a part of the model of intrusion alerts with predefined alert classes, comprises using a machine learning technique, such as a neural network, a support vector machine, decision trees or a combination of them. It may be advantageous to use a machine learning technique as it enables automatic profiling of the data in relation to the alerts and automatic comparison.

In yet another embodiment the intrusion alerts are classified in a "false" class or a "true" class. It may be advantageous to classify the data in relation to the alert as being a true or a false alert, in order to limit the number of alerts generated by the ABS that are not related to an attack.

According to the invention a system is provided to perform the method described above in order to classify intrusion alerts. The system for classifying intrusion alerts in a computer network comprises an intrusion detection system arranged for monitoring traffic data in the computer network, for detecting an occurrence of an intrusion from the monitored traffic data and for providing in response to the detection of the occurrence of the intrusion, an intrusion alert and data in relation to the intrusion alert, an alert information extractor arranged for generating a statistical analysis of the data in relation to the intrusion alert, and an alert classification engine arranged for classifying the intrusion alert based on said statistical analysis.

In another embodiment of the invention, the intrusion detection system further comprises a traffic data monitor for monitoring traffic data in a computer network, an anomaly detector for detecting an anomaly on a basis of said monitoring and a model describing normal traffic data in a computer network, and an alert generator for providing in response to the detection of anomaly, an intrusion alert and for providing data in relation to the intrusion alert.

Brief description of the drawings

Further advantageous embodiments of the assembly according to the invention are described in the claims and in the following description with reference to the drawing, in which:

Figure 1 depicts a flow diagram of a process for classifying intrusion alerts in a computer network, illustrative for some embodiments according to the invention, in a working mode;

Figure 2 depicts a flow diagram of a process for classifying intrusion alerts in a computer network, illustrative for some embodiments according to the invention, in a training mode;

Figure 3 depicts a highly schematic diagram of a system for classifying intrusion alerts in a computer network, illustrative for some embodiments according to the invention, in a working mode.

Figure 4 depicts a highly schematic diagram of a system for classifying intrusion alerts in a computer network, illustrative for some embodiments according to the invention, in a training mode.

Detailed description of the invention

In figure 1 a flow diagram of a process for classifying intrusion alerts in a computer network, illustrative for some embodiments according to the invention is shown in a working mode. In the working mode, a model of intrusion alerts with predefined alert classes is present and has already been generated. The generation of the model is described further below. In the working mode, classification of an intrusion alert will start by monitoring traffic data in a computer network, step a in figure 1.

Next step is detecting an occurrence of an intrusion from the monitored traffic data (step b). Detecting an intrusion may be achieved by an anomaly-based intrusion detection system or by any other intrusion detection system. In figure 1, steps a, b,, c, are normally performed by an anomaly-based intrusion detection system. Detection of an anomaly (step b) then implies that traffic data has been identified as deviating significantly from normal network traffic data. Then an alert and data in relation to the alert will be provided (step c).

The data in relation to the intrusion alert may comprise the attack payload that had triggered the (anomaly-based) intrusion detection system to generate the alert or it may be data representative of this payload.

The next step, step d in figure 1, is generating a statistical analysis of the data in relation to the alert, which will be the basis of the classification. The generation of the statistical analysis may be accomplished by an alert information extractor (AIE). The analysis should incorporate enough features from the original data to distinguish alerts belonging to

different classes. Furthermore, the analysis should be efficient with respect to the required resources of the alert information extractor. For example, if the generating of the statistical analysis requires too much memory space or/and computing power, the alert information extractor may be become too slow or too resource consuming.

According to an embodiment of the invention, the generation of the statistical analysis is achieved using n-gram analysis. N-gram analysis is a technique used to profile for example the payload content by marking the occurrence (and, additionally, the frequency) of n-grams, where n-grams may be sequence of n bytes. For example, a 1-gram analysis can be used, where average byte frequency and standard deviation values of payloads are stored. It is also possible to use higher order n-grams, i.e., n-grams where n>1. The memory space needed to store average and standard deviation values for each n-gram grows exponentially (e.g., 640GB would be needed to store 5-grams statistics). Another possibility is to store the fact that a certain n-gram has occurred, rather than computing average byte frequency and standard deviation statistics. This may be advantageous because high-order n-grams are more sparse than low-order n-grams, thus it is more difficult to gather accurate statistics (i.e., with a sufficient number of samples) as the order increases. Another advantage may be that it requires less space in memory.

The amount of data resulting from the statistical analysis can be stored in different ways, for example using a bitmap data structure. Another way of storing the data compactly is applying a Bloom filter on the data. A Bloom filter yields a bit array of m bits, where m can be any integer number. Like a bitmap, it stores binary information.

The step of classifying the intrusion alerts based on the statistical analysis, step e, may comprise two steps, i.e. comparing at least a part of the statistical analysis with at least a part of a model of intrusion alerts with predefined alert classes (step e1) and assigning one of the predefined alert classes to the intrusion alert based on the comparison (step e2).

To understand the content of the model of intrusion alerts with predefined alert classes, the generating the model is discussed first. In figure 2, a flow diagram of a for classifying intrusion alerts in a computer network, illustrative for some embodiments according to the invention is depicted in a training mode. In the training mode the model of intrusion alerts with predefined alert classes is generated.

First, a training set of is provided. This data can be delivered directly to the process of generating a statistical analysis when it contains the required data in relation to the alerts. However, it is also possible to provide a training set of traffic data to an anomaly-based intrusion system. This is shown in figure 2 in step aa1. The anomaly-based intrusion system may then monitor the traffic data (step a), detect an intrusion (step b), provide an alert and

data in relation to the alert (step c) to the alert information extractor. In this way the data in relation to the alert is automatically generated.

Just as in working mode, a statistical analysis of the data in relation to the alert is generated (step aa2). The statistical analysis will be matched with one or more classes (step aa3). These classes of intrusion alerts have been predefined (step aa3). A machine learning technique may be used for identifying the classes in the statistical analysis of data in relation to the intrusion alerts. Since the alert classes, the alerts, and the data related to such alerts are well known, classes can be assigned to the statistical analysis. Then a model of intrusion alerts with predefined alert classes can be constructed (aa5). The model serves as a reference when classifying intrusion alerts in the working mode.

The predefined classes are identified either on the basis of a signature based intrusion detection system (step f2) and/or by a human operator (step f1). In case a signature-based intrusion detection system is used, it has to monitor the same training set of traffic data. The signature-based intrusion detection may identify attacks in the training set of traffic data, raise alerts, and also identify the classes of the attacks which caused the alerts. The work load for the security team members may be low, but the classification accuracy may also be low.

Another possibility is that a human operator classifies the alerts raised by the anomaly-based intrusion detection system. Although this requires human intervention, it may produce better results, since each alert is consistently classified. A combination of two methods is also possible, when the human operator may classify the alerts in a consistent manner with the signature-based intrusion detection.

In the working mode, the model of intrusion alerts with predefined alert classes is used to classify the alerts. This may be executed by the so called alert classification engine. The statistical analysis of the data in relation to the alert is compared with the model (figure 1, step e1) and on the basis of the comparison, one of the predefined alert classes is assigned to the intrusion alert (step e2). Any supervised machine learning technique, such as a neural network, a support vector machine or decision trees, may be used for this.

In another embodiment of the invention, the alert classification engine may assign all alerts to either a "false" class or a "true" class. It may be advantageous to use the invention to distinguish true attacks from false attacks.

In figure 3, a highly schematic diagram of a system for classifying intrusion alerts in a computer network, illustrative for some embodiments according to the invention is depicted in a working mode. It depicts an intrusion detection system (IDS) g1, which may monitor traffic data between an (external) network g4, for example the internet, and a network that has to be protected against attacks, such as LAN network g5. It further depicts an alert information extractor (AIE) g2 that is arranged for executing the steps d and aa2 as

mentioned above. The data in relation to the alert may, according to an embodiment of the invention, be provided by an anomaly-based intrusion detection system e3, arranged for executing steps a and a, b and c as described above.

The statistical analysis of the data in relation to the alert is provided by the alert information extractor (AIE) g2 to the alert classification engine (ACE) g3. The alert classification engine is arranged to execute steps e, e1, e2 and aa4, aa5 as mentioned above.

In figure 4 a highly schematic diagram of a system for classifying intrusion alerts in a computer network, illustrative for some embodiments according to the invention is depicted in a training mode. A data set provider h1 is arranged to execute step aa1 as mentioned above or to provide data in relation to the alerts directly to the AIE, g2. Also a signature-based intrusion detection system h2 and a human operator h3 are shown and arranged to executed the steps that are described above.

Referring to the preceding explanation of the invention, it is noted that further modifications and embodiments are very well conceivable. Also further modifications and embodiments are within the scope of this invention.

CLAIMS

1. A method for classifying intrusion alerts in a computer network, comprising the steps of
   a) monitoring traffic data in a computer network;
   b) detecting an occurrence of an intrusion from the monitored traffic data
   c) providing in response to the detection of the occurrence of the intrusion, an intrusion alert and data in relation to the intrusion alert;
   d) generating a statistical analysis of the data in relation to the intrusion alert; and,
   e) classifying the intrusion alert based on said statistical analysis.

2. The method according to claim 1, wherein step b) comprises
   b1) detecting an anomaly on a basis of said monitoring and a model describing normal traffic data in a computer network.

3. The method according to one of claims 1 or 2, wherein the data in relation to the intrusion alert comprises at least one payload of the traffic data that caused the intrusion alert.

4. The method according to one of claims 1-3, wherein step b) comprises generating information about a statistical distribution of n-grams in at least a part of the data in relation to the intrusion alert

5. The method according to claim 4, wherein the n-grams are sequences of bytes.

6. The method according to one of claims 1-3, wherein step b) comprises generating information about byte frequency in at least a part of the data in relation to the intrusion alert.

7. The method according to one of claims 3-6, wherein step b) comprises applying a bloom filter on the statistical distribution of n-grams or storing the statistical distribution of n-grams in bitmap data structures.

8. The method according to one of claims 1-7, wherein step e) comprises
   e1) comparing at least a part of the statistical analysis with at least a part of a model of intrusion alerts with predefined alert classes; and,
   e2) assigning one of the predefined alert classes to the intrusion alert based on the comparison.

9. The method according to claim 8, further comprising, before step a)
aa) generating a model of intrusion alerts with predefined alert classes.

10. The method according to claim 9, wherein step aa) comprises the steps of
aa1) providing a training set of data in relation to intrusion alerts;
aa2) generating a statistical analysis of said training set of data;
aa3) predefining at least two alert classes; and,
aa4) assigning predefined alert classes to one or more parts of said statistical analysis, based on information provided by a signature-based intrusion detection system, and/or by a human operator;
aa5) constructing a model of intrusion alerts comprising one or more parts of said statistical analysis and hereto assigned predefined alert classes.

11. The method according to one of claims 8-10, wherein step e1) comprises using a machine learning technique.

12. The method according to claims 11, wherein the machine learning technique comprises a neural network, a support vector machine and/or decision trees.

13. The method according to one of claims 1-12, wherein the intrusion alert are classified in a "false" class or a "true" class.

14. A system for classifying intrusion alerts in a computer network, comprising
- an intrusion detection system arranged for monitoring traffic data in the computer network, for detecting an occurrence of an intrusion from the monitored traffic data and for providing in response to the detection of the occurrence of the intrusion, an intrusion alert and data in relation to the intrusion alert,
- an alert information extractor arranged for generating a statistical analysis of the data in relation to the intrusion alert; and
- an alert classification engine arranged for classifying the intrusion alert based on said statistical analysis.

15. The system according to claim 14, wherein the intrusion detection system further comprises

a traffic data monitor for monitoring traffic data in the computer network;

an anomaly detector for detecting an anomaly on a basis of said monitoring and a model describing normal traffic data in the computer network; and

an alert generator for providing in response to the detection of anomaly, an intrusion alert and for providing data in relation to the intrusion alert.

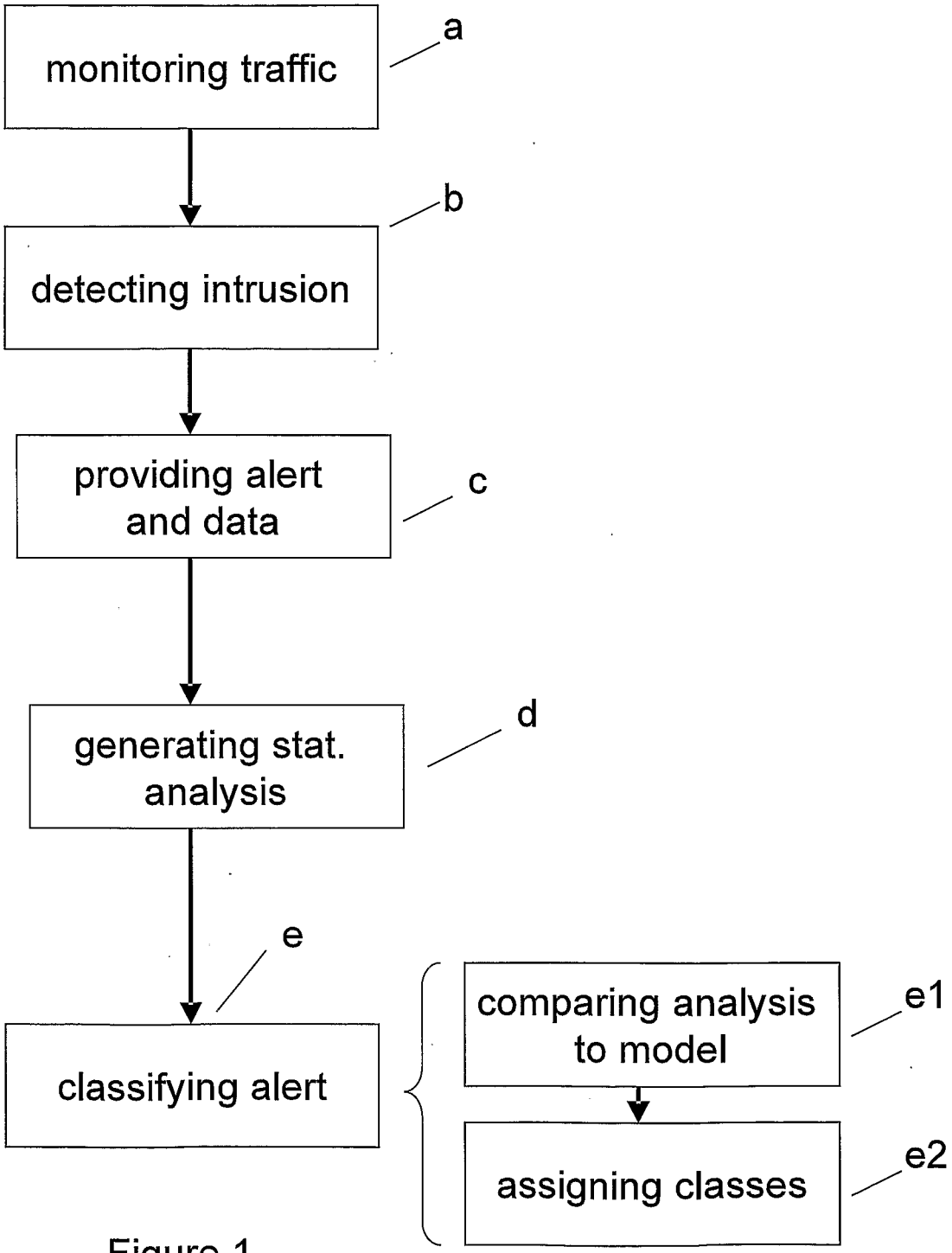
monitoring traffic
a
detecting intrusion
b
providing alert and data
c
generating stat. analysis
d
e
classifying alert
comparing analysis to model
e1
assigning classes
e2

Figure 1

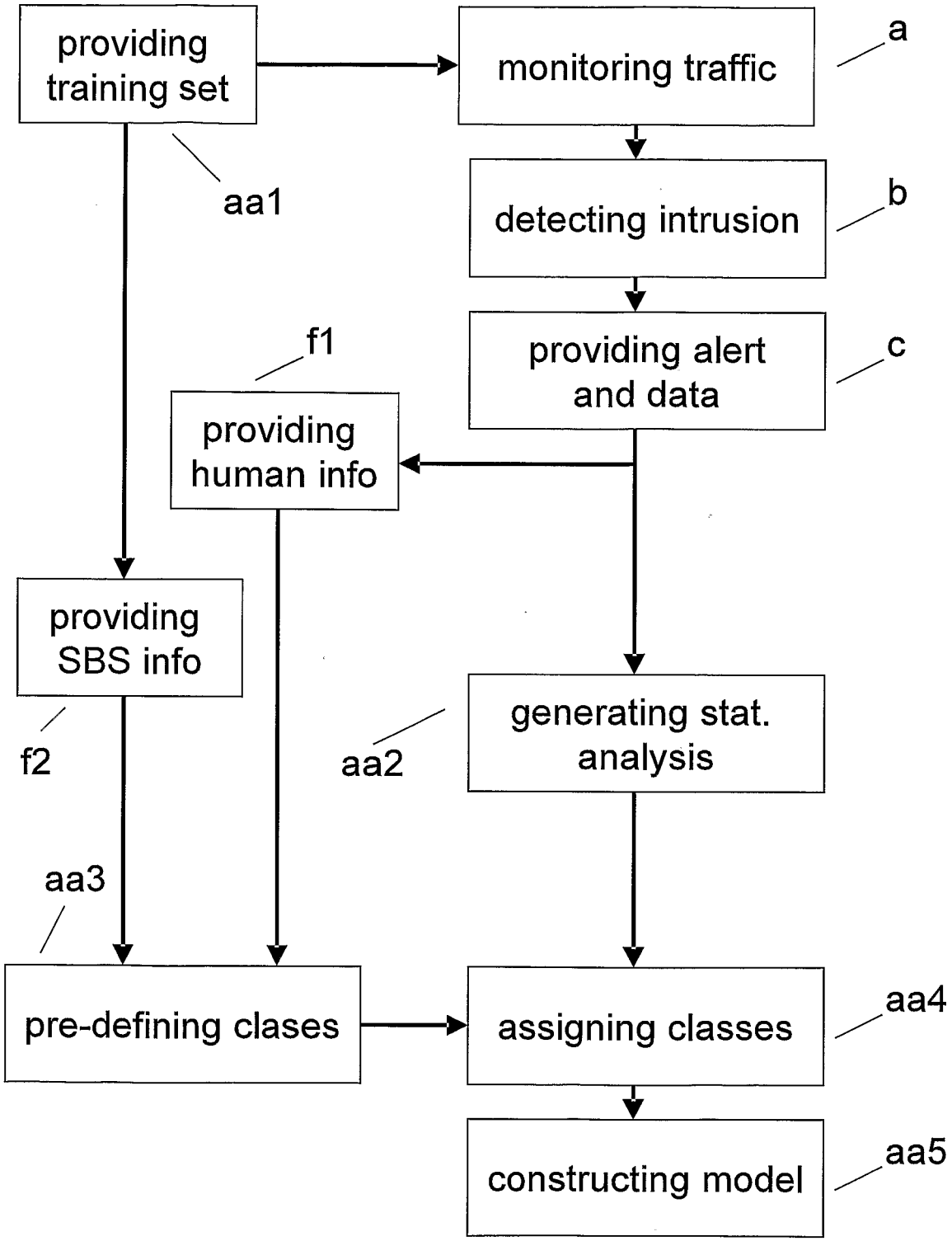
providing training set
monitoring traffic
a
aa1
detecting intrusion
b
providing alert and data
c
f1
providing human info
providing SBS info
f2
aa2
generating stat. analysis
aa3
pre-defining clases
assigning classes
aa4
constructing model
aa5

Figure 2

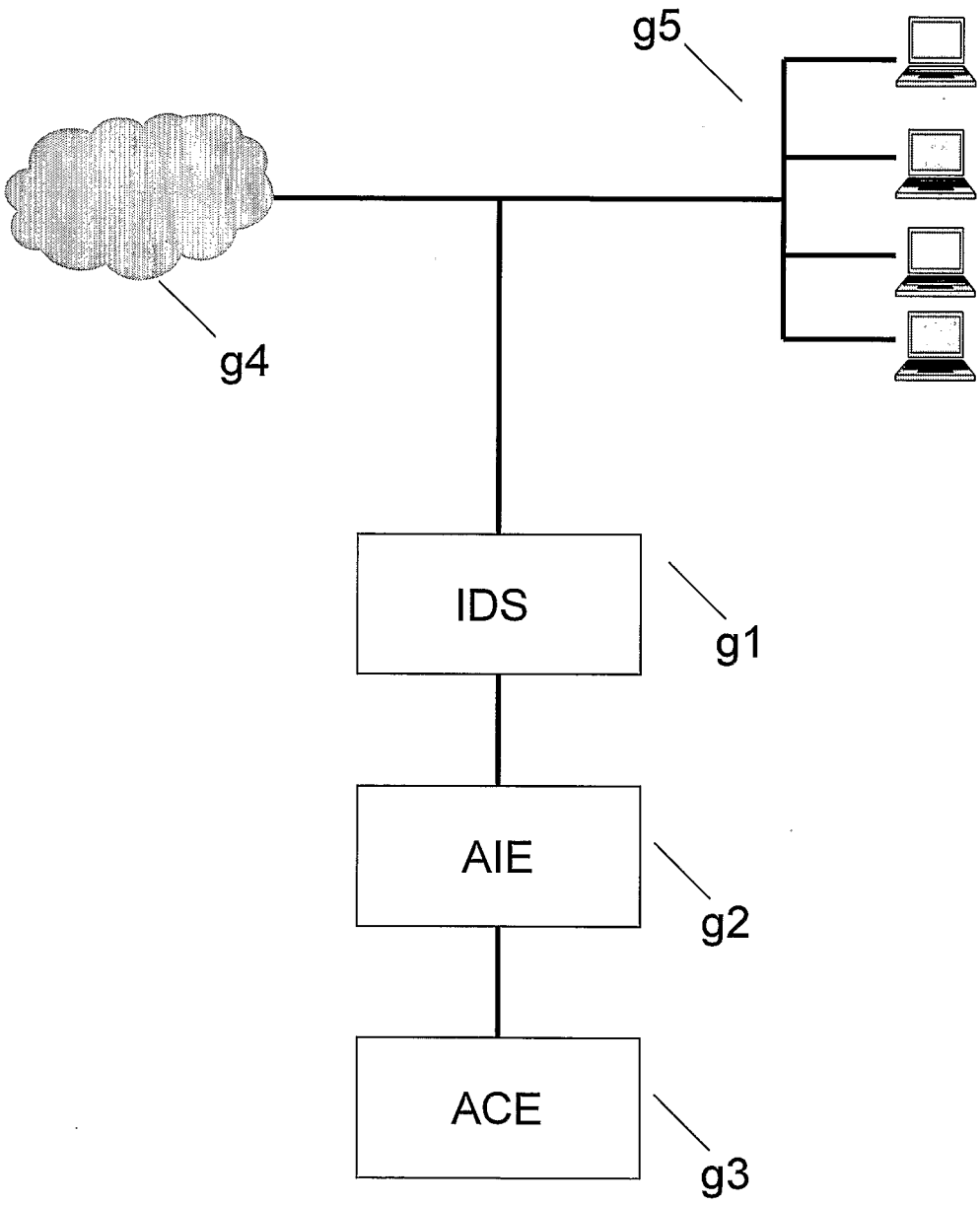

Figure 3

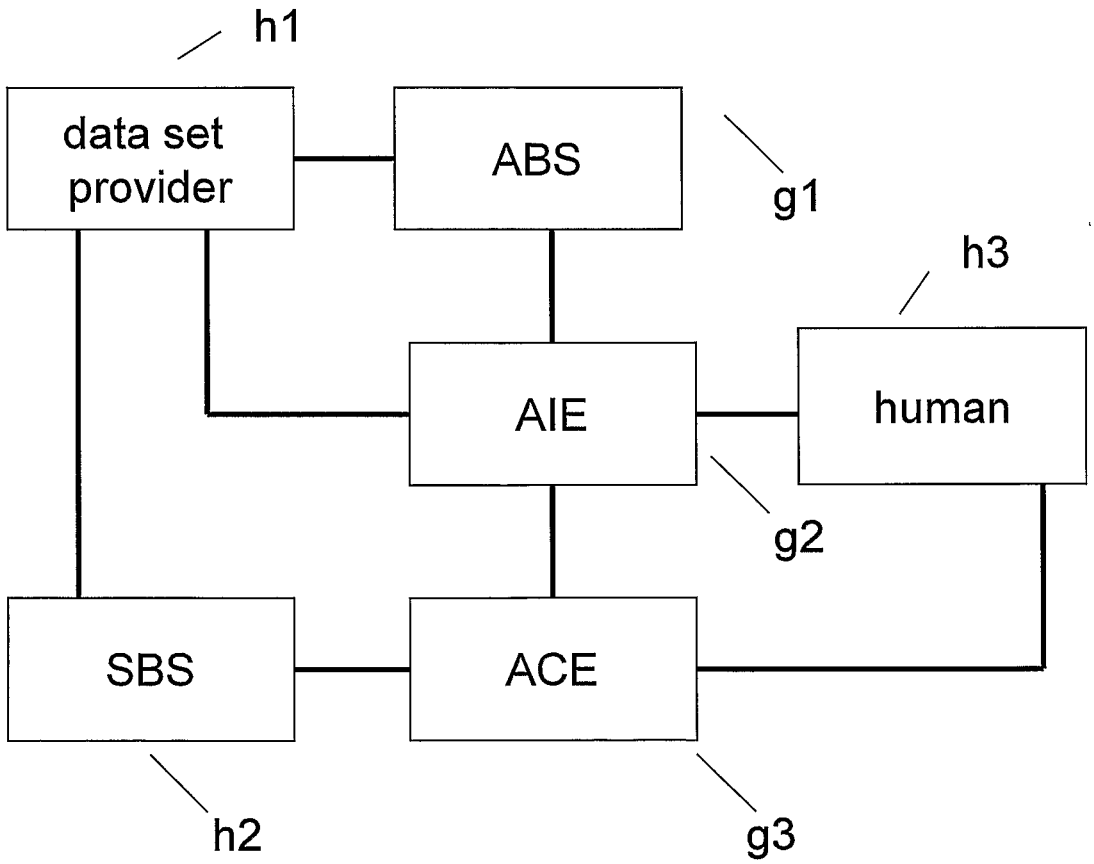

Figure 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/NL2010/000060

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04L12/24
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007/118905 A1 (MORIN BENJAMIN [FR] ET AL) 24 May 2007 (2007-05-24) cited in the application paragraphs [0029] - [0045]	1-15
X	US 2007/150954 A1 (SHON TAE-SHIK [KR]) 28 June 2007 (2007-06-28) paragraphs [0014] - [0016], [0079], [0084]	1-15
A	US 2005/060295 A1 (GOULD STEPHEN [AU] ET AL) 17 March 2005 (2005-03-17) paragraphs [0017] - [0019]	1-15

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 June 2010	22/06/2010

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Fax: (+31–70) 340–3016	Veen, Gerardus

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/NL2010/000060

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007118905 A1	24-05-2007	AT 358373 T	15-04-2007
		DE 602004005616 T2	24-01-2008
		EP 1695485 A2	30-08-2006
		FR 2864392 A1	24-06-2005
		WO 2005060160 A2	30-06-2005
US 2007150954 A1	28-06-2007	JP 2007179542 A	12-07-2007
		KR 20070068845 A	02-07-2007
US 2005060295 A1	17-03-2005	NONE	