available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Anomaly-based network intrusion detection: Techniques, systems and challenges

P. García-Teodoro[a,*], J. Díaz-Verdejo[a], G. Maciá-Fernández[a], E. Vázquez[b]

[a]Department of Signal Theory, Telematics and Communications – Computer Science and Telecommunications Faculty, University of Granada, Granada, Spain

[b]Department of Telematic Engineering - Universidad Politécnica de Madrid, Madrid, Spain

ARTICLE INFO

Article history:
Received 9 January 2008
Accepted 13 August 2008

Keywords:
Network security
Threat
Intrusion detection
Anomaly detection
IDS systems and platforms
Assessment

ABSTRACT

The Internet and computer networks are exposed to an increasing number of security threats. With new types of attacks appearing continually, developing flexible and adaptive security oriented approaches is a severe challenge. In this context, anomaly-based network intrusion detection techniques are a valuable technology to protect target systems and networks against malicious activities. However, despite the variety of such methods described in the literature in recent years, security tools incorporating anomaly detection functionalities are just starting to appear, and several important problems remain to be solved. This paper begins with a review of the most well-known anomaly-based intrusion detection techniques. Then, available platforms, systems under development and research projects in the area are presented. Finally, we outline the main challenges to be dealt with for the wide scale deployment of anomaly-based intrusion detectors, with special emphasis on assessment issues.

1. Introduction

Intrusion Detection Systems (IDS) are security tools that, like other measures such as antivirus software, firewalls and access control schemes, are intended to strengthen the security of information and communication systems. Although, as shown in Kabiri and Ghorbani (2005) and Sobh (2006), several IDS approaches have been proposed in the specialized literature since the origins of this technology, two highly relevant works in this direction are Denning (1987) and Staniford-Chen et al. (1998).

Noteworthy work has been carried out by CIDF (“Common Intrusion Detection Framework”), a working group created by DARPA in 1998 mainly oriented towards coordinating and defining a common framework in the IDS field. Integrated within IETF in 2000, and having adopted the new acronym IDWG (“Intrusion Detection Working Group”), the group defined a general IDS architecture based on the consideration of four types of functional modules (Fig. 1):

- *E blocks* (“Event-boxes”): This kind of block is composed of sensor elements that monitor the target system, thus acquiring information events to be analyzed by other blocks.
- *D blocks* (“Database-boxes”): These are elements intended to store information from E blocks for subsequent processing by A and R boxes.
- *A blocks* (“Analysis-boxes”): Processing modules for analyzing events and detecting potential hostile behaviour, so that some kind of alarm will be generated if necessary.

* *Corresponding author*. Department of Signal Theory, Telematics and Communications – Computer Science and Telecommunications Faculty, University of Granada, C/ Periodista Daniel Saucedo Aranda, 18071 Granada, Spain. Tel.: +34 958242305; fax: +34 958240831.
E-mail addresses: pgteodor@ugr.es (P. García-Teodoro), jedv@ugr.es (J. Díaz-Verdejo), gmacia@ugr.es (G. Maciá-Fernández), enrique@dit.upm.es (E. Vázquez).

0167-4048/$ – see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2008.08.003

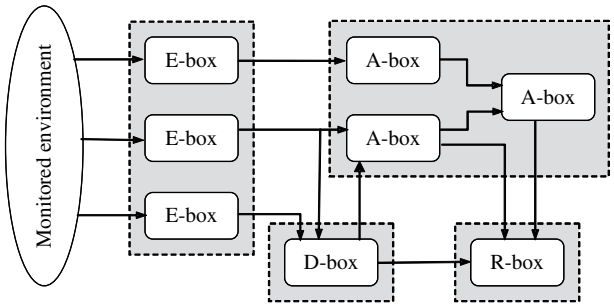

Fig. 1 – General CIDF architecture for IDS systems.

- *R blocks* (''Response-boxes''): The main function of this type of block is the execution, if any intrusion occurs, of a response to thwart the detected menace.

Other key contributions in the IDS field concern the definition of protocols for data exchange between components (e.g. IDXP, ''Intrusion Detection eXchange Protocol'', RFC 4767), and the format considered for this (e.g. IDMEF, ''Intrusion Detection MEssage Format'', RFC 4765).

Depending on the information source considered (E boxes in Fig. 1), an IDS may be either host or network-based. A host-based IDS analyzes events such as process identifiers and system calls, mainly related to OS information. On the other hand, a network-based IDS analyzes network related events: traffic volume, IP addresses, service ports, protocol usage, etc. This paper focuses on the latter type of IDS.

Depending on the type of analysis carried out (A blocks in Fig. 1), intrusion detection systems are classified as either signature-based or anomaly-based. Signature-based schemes (also denoted as misuse-based) seek defined patterns, or *signatures*, within the analyzed data. For this purpose, a signature database corresponding to known attacks is specified a priori. On the other hand, anomaly-based detectors attempt to estimate the ''normal'' behaviour of the system to be protected, and generate an anomaly alarm whenever the deviation between a given observation at an instant and the normal behaviour exceeds a predefined threshold. Another possibility is to model the ''abnormal'' behaviour of the system and to raise an alarm when the difference between the observed behaviour and the expected one falls below a given limit.

Signature and anomaly-based systems are similar in terms of conceptual operation and composition. The main differences between these methodologies are inherent in the concepts of ''attack'' and ''anomaly''. An attack can be defined as ''a sequence of operations that puts the security of a system at risk''. An anomaly is just ''an event that is suspicious from the perspective of security''. Based on this distinction, the main advantages and disadvantages of each IDS type can be pointed out.

Signature-based schemes provide very good detection results for specified, well-known attacks. However, they are not capable of detecting new, unfamiliar intrusions, even if they are built as minimum variants of already known attacks. On the contrary, the main benefit of anomaly-based detection techniques is their potential to detect previously unseen intrusion events. However, and despite the likely inaccuracy in formal signature specifications, the rate of false positives (or FP, events erroneously classified as attacks; see Section 2) in anomaly-based systems is usually higher than in signature-based ones.

Given the promising capabilities of anomaly-based network intrusion detection systems (A-NIDS), this approach is currently a principal focus of research and development in the field of intrusion detection. Various systems with A-NIDS capabilities are becoming available, and many new schemes are being explored. However, the subject is far from mature and key issues remain to be solved before wide scale deployment of A-NIDS platforms can be practicable.

Focusing, thus, on A-NIDS technologies, the rest of this paper is organized as follows: Section 2 presents the various algorithms proposed for anomaly detection. Then, existing A-NIDS platforms, either currently available or under development, and which include anomaly detection functionalities, are presented in Section 3. This constitutes a valuable contribution of the present paper in comparison with other published work. The fourth section discusses open issues and challenges in this field, with special emphasis on A-NIDS assessment. Finally, Section 5 summarizes the main points of the paper.

2. A-NIDS techniques

Although different A-NIDS approaches exist (Estévez-Tapiador et al., 2004), in general terms all of them consist of the following basic modules or stages (Fig. 2):

- *Parameterization*: In this stage, the observed instances of the target system are represented in a pre-established form.
- *Training* stage: The normal (or abnormal) behaviour of the system is characterized and a corresponding model is built. This can be done in very different ways, automatically or manually, depending on the type of A-NIDS considered (see classification below).
- *Detection* stage: Once the model for the system is available, it is compared with the (parameterized) observed traffic. If the deviation found exceeds (or is below, in the case of abnormality models) a given threshold an alarm will be triggered (Estévez-Tapiador et al., 2004).

According to the type of processing related to the ''behavioural'' model of the target system, anomaly

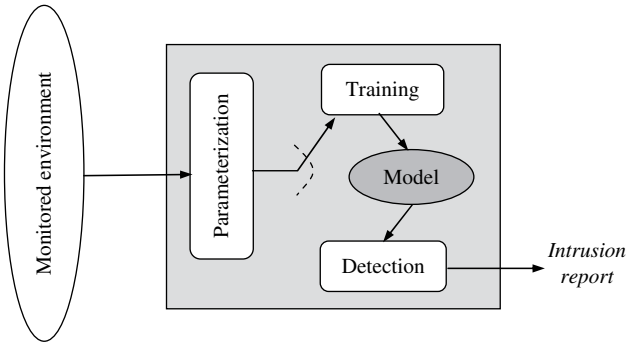

Fig. 2 – Generic A-NIDS functional architecture.

detection techniques can be classified into three main categories (Lazarevic et al., 2005) (see Fig. 3): *statistical-based*, *knowledge-based*, and *machine learning-based*. In the statistical-based case, the behaviour of the system is represented from a random viewpoint. On the other hand, knowledge-based A-NIDS techniques try to capture the claimed behaviour from available system data (protocol specifications, network traffic instances, etc.). Finally, machine learning A-NIDS schemes are based on the establishment of an explicit or implicit model that allows the patterns analyzed to be categorized.

Two key aspects concern the evaluation, and thus the comparison, of the performance of alternative intrusion detection approaches: these are the efficiency of the detection process, and the cost involved in the operation. Without underestimating the importance of the cost, at this point the efficiency aspect must be emphasized. Four situations exist in this context, corresponding to the relation between the result of the detection for an analyzed event (''normal'' *vs.* ''intrusion'') and its actual nature (''innocuous'' *vs.* ''malicious''). These situations are: *false positive* (FP), if the analyzed event is innocuous (or ''clean'') from the perspective of security, but it is classified as malicious; *true positive* (TP), if the analyzed event is correctly classified as intrusion/malicious; *false negative* (FN), if the analyzed event is malicious but it is classified as normal/innocuous; and *true negative* (TN), if the analyzed event is correctly classified as normal/innocuous. It is clear that low FP and FN rates, together with high TP and TN rates, will result in good efficiency values.

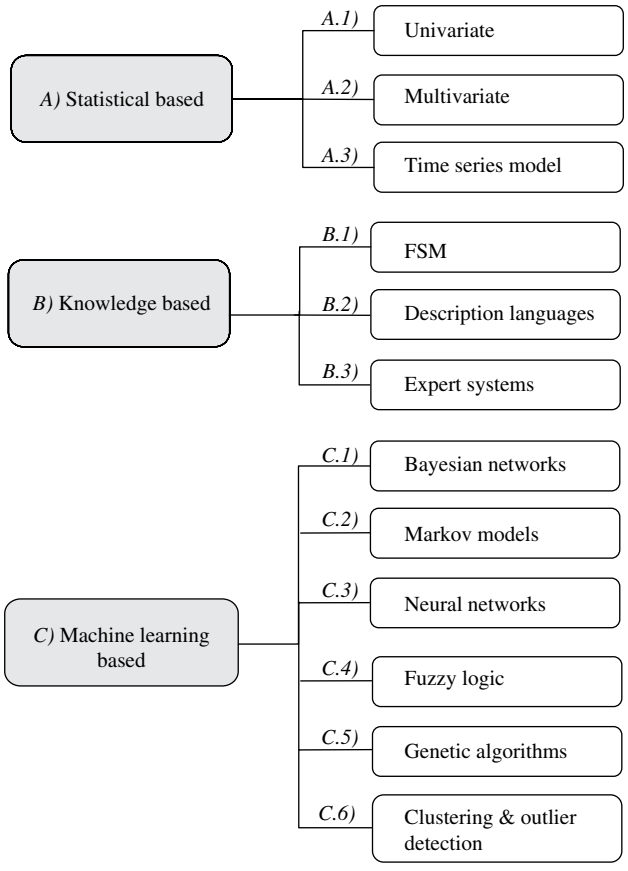

Fig. 3 – Classification of the anomaly detection techniques according to the nature of the processing involved in the ''behavioural'' model considered.

The fundamentals for statistical, knowledge and machine learning-based A-NIDS, as well as the principal subtypes of each, are described below. The main features of all are summarized in Table 1. Above and beyond other possibilities, the question of efficiency should be a prime consideration in selecting and implementing A-NIDS methodologies.

2.1. *Statistical-based A-NIDS techniques*

In statistical-based techniques, the network traffic activity is captured and a profile representing its stochastic behaviour is created. This profile is based on metrics such as the traffic rate, the number of packets for each protocol, the rate of connections, the number of different IP addresses, etc. Two datasets of network traffic are considered during the anomaly detection process: one corresponds to the currently observed profile over time, and the other is for the previously trained statistical profile. As the network events occur, the current profile is determined and an anomaly score estimated by comparison of the two behaviours. The score normally indicates the degree of irregularity for a specific event, such that the intrusion detection system will flag the occurrence of an anomaly when the score surpasses a certain threshold.

The earliest statistical approaches, both network oriented and host oriented IDS, corresponded to univariate models, which modelled the parameters as independent Gaussian random variables (Denning and Neumann, 1985), thus defining an acceptable range of values for every variable. Later, multivariate models that consider the correlations between two or more metrics were proposed (Ye et al., 2002). These are useful because experimental data have shown that a better level of discrimination can be obtained from combinations of related measures rather than individually. Other studies have considered time series models (Detecting Hackers), which use an interval timer, together with an event counter or resource measure, and take into account the order and the inter-arrival times of the observations as well as their values. Thus, an observed traffic instance will be labelled as abnormal if its probability of occurrence is too low at a given time.

Apart from their inherent features for use as anomaly-based techniques, statistical A-NIDS approaches have a number of virtues. Firstly, they do not require prior knowledge about the normal activity of the target system; instead, they have the ability to learn the expected behaviour of the system from observations. Secondly, statistical methods can provide accurate notification of malicious activities occurring over long periods of time.

However, some drawbacks should also be pointed out. First, this kind of A-NIDS is susceptible to be trained by an attacker in such a way that the network traffic generated during the attack is considered as normal. Second, setting the values of the different parameters/metrics is a difficult task, especially because the balance between false positives and false negatives is affected. Moreover, a statistical distribution per variable is assumed, but not all behaviours can be

Table 1 – Fundamentals of the A-NIDS techniques

Technique: *basics*	■ Pros ■ Cons	Subtypes
A) Statistical-based: *stochastic behaviour*	■ Prior knowledge about normal activity not required. Accurate notification of malicious activities. ■ Susceptible to be trained by attackers. Difficult setting for parameters and metrics. Unrealistic quasi-stationary process assumption.	A.1) Univariate models *(independent Gaussian random variables)* A.2) Multivariate models *(correlations among several metrics)* A.3) Time series *(interval timers, counters and some other time-related metrics)*
B) Knowledge-based: *availability of prior knowledge/data*	■ Robustness. Flexibility and scalability. ■ Difficult and time-consuming availability for high-quality knowledge/data.	B.1) Finite state machines *(states and transitions)* B.2) Description languages *(N-grams, UML, …)* B.3) Expert systems *(rules-based classification)*
C) Machine learning-based: *categorization of patterns*	■ Flexibility and adaptability. Capture of interdependencies. ■ High dependency on the assumption about the behaviour accepted for the system. High resource consuming.	C.1) Bayesian networks *(probabilistic relationships among variables)* C.2) Markov models *(stochastic Markov theory)* C.3) Neural networks *(human brain foundations)* C.4) Fuzzy logic *(approximation and uncertainty)* C.5) Genetic algorithms *(evolutionary biology inspired)* C.6) Clustering and outlier detection *(data grouping)*

modelled by using stochastic methods. Furthermore, most of these schemes rely on the assumption of a quasi-stationary process, which is not always realistic.

2.2. *Knowledge-based techniques*

The so-called expert system approach is one of the most widely used knowledge-based IDS schemes. However, like other A-NIDS methodologies, expert systems can also be classified into other, different categories (Denning and Neumann, 1985; Anderson et al., 1995). Expert systems are intended to classify the audit data according to a set of rules, involving three steps. First, different attributes and classes are identified from the training data. Second, a set of classification rules, parameters or procedures are deduced. Third, the audit data are classified accordingly.

More restrictive/particular in some senses are specification-based anomaly methods, for which the desired model is manually constructed by a human expert, in terms of a set of rules (the specifications) that seek to determine legitimate system behaviour. If the specifications are complete enough, the model will be able to detect illegitimate behavioural patterns. Moreover, the number of false positives is reduced, mainly because this kind of system avoids the problem of harmless activities, not previously observed, being reported as intrusions.

Specifications could also be developed by using some kind of formal tool. For example, the finite state machine (FSM) methodology –a sequence of states and transitions among them– seems appropriate for modelling network protocols (Estévez-Tapiador et al., 2003). For this purpose, standard description languages such as *N*-grammars, UML and LOTOS can be considered.

The most significant advantages of current approaches to anomaly detection are those of robustness and flexibility. Their main drawback is that the development of high-quality knowledge is often difficult and time-consuming (Sekar et al., 2002). This problem, however, is common to other A-NIDS methods for which the notion of normality is obtained exclusively by analyzing training data .

2.3. *Machine learning-based A-NIDS schemes*

Machine learning techniques are based on establishing an explicit or implicit model that enables the patterns analyzed to be categorized. A singular characteristic of these schemes is the need for labelled data to train the behavioural model, a procedure that places severe demands on resources.

In many cases, the applicability of machine learning principles coincides with that for the statistical techniques, although the former is focused on building a model that improves its performance on the basis of previous results. Hence, a machine learning A-NIDS has the ability to change its execution strategy as it acquires new information. Although this feature could make it desirable to use such schemes for all situations, the major drawback is their resource expensive nature.

Several machine learning-based schemes have been applied to A-NIDS. Some of the most important are cited below, and their main advantages and drawbacks are identified.

2.3.1. *Bayesian networks*

A Bayesian network is a model that encodes probabilistic relationships among variables of interest. This technique is generally used for intrusion detection in combination with statistical schemes, a procedure that yields several advantages (Heckerman, 1995), including the capability of encoding interdependencies between variables and of predicting events, as well as the ability to incorporate both prior knowledge and data.

However, as pointed out in Kruegel et al. (2003), a serious disadvantage of using Bayesian networks is that their results are similar to those derived from threshold-based systems, while considerably higher computational effort is required.

Although the use of Bayesian networks has proved to be effective in certain situations, the results obtained are highly dependent on the assumptions about the behaviour of the target system, and so a deviation in these hypotheses leads to detection errors, attributable to the model considered.

2.3.2. *Markov models*

Within this category, we may distinguish two main approaches: Markov chains and hidden Markov models. A Markov chain is a set of states that are interconnected through certain transition probabilities, which determine the topology and the capabilities of the model. During a first training phase, the probabilities associated to the transitions are estimated from the normal behaviour of the target system. The detection of anomalies is then carried out by comparing the anomaly score (associated probability) obtained for the observed sequences with a fixed threshold.

In the case of a hidden Markov model, the system of interest is assumed to be a Markov process in which states and transitions are hidden. Only the so-called productions are observable.

Markov-based techniques have been extensively used in the context of host IDS, normally applied to system calls (Yeung and Ding, 2003). In network IDS, the inspection of packets has led to the use of Markov models in some approaches (Mahoney and Chan, 2002; Estévez-Tapiador et al., 2005). In all cases, the model derived for the target system has provided a good approach for the claimed profile, while, as in Bayesian networks, the results are highly dependent on the assumptions about the behaviour accepted for the system.

2.3.3. *Neural networks*

With the aim of simulating the operation of the human brain (featuring the existence of neurons and of synapses among them), neural networks have been adopted in the field of anomaly intrusion detection, mainly because of their flexibility and adaptability to environmental changes. This detection approach has been employed to create user profiles (Fox et al., 1990), to predict the next command from a sequence of previous ones (Debar et al., 1992), to identify the intrusive behaviour of traffic patterns (Cansian et al., 1997), etc.

However, a common characteristic in the proposed variants, from recurrent neural networks to self-organizing maps (Ramadas et al., 2003), is that they do not provide a descriptive model that explains why a particular detection decision has been taken.

2.3.4. *Fuzzy logic techniques*

Fuzzy logic is derived from fuzzy set theory under which reasoning is approximate rather than precisely deduced from classical predicate logic. Fuzzy techniques are thus used in the field of anomaly detection mainly because the features to be considered can be seen as fuzzy variables (Bridges and Vaughn, 2000). This kind of processing scheme considers an observation as normal if it lies within a given interval (Dickerson, 2000).

Although fuzzy logic has proved to be effective, especially against port scans and probes, its main disadvantage is the high resource consumption involved. On the other hand, it should also be noticed that fuzzy logic is controversial in some circles, and it has been rejected by some engineers and by most statisticians, who hold that probability is the only rigorous mathematical description of uncertainty.

2.3.5. *Genetic algorithms*

Genetic algorithms are categorized as global search heuristics, and are a particular class of evolutionary algorithms (also known as evolutionary computation) that use techniques inspired by evolutionary biology such as inheritance, mutation, selection and recombination. Thus, genetic algorithms constitute another type of machine learning-based technique, capable of deriving classification rules (Li, 2004) and/or selecting appropriate features or optimal parameters for the detection process (Bridges and Vaughn, 2000).

The main advantage of this subtype of machine learning A-NIDS is the use of a flexible and robust global search method that converges to a solution from multiple directions, whilst no prior knowledge about the system behaviour is assumed. Its main disadvantage is the high resource consumption involved.

2.3.6. *Clustering and outlier detection*

Clustering techniques work by grouping the observed data into clusters, according to a given similarity or distance measure. The procedure most commonly used for this consists in selecting a representative point for each cluster. Then, each new data point is classified as belonging to a given cluster according to the proximity to the corresponding representative point (Portnoy et al., 2001). Some points may not belong to any cluster; these are named outliers and represent the anomalies in the detection process.

Clustering and outliers are used at present in the field of IDS (Barnett and Lewis, 1994; Sequeira and Zaki, 2002), with several variants depending on how the question ''Is the isolated outlier an anomaly?'' is answered. For example, the KNN (k-nearest neighbour) approach (Liao and Vemuri, 2002) uses the Euclidean distance to define the membership of data points to a given cluster, while other systems use the Mahalanobis distance. Some detection proposals associate a certain degree of being an outlier for each point (Breunig et al., 2000).

Clustering techniques determine the occurrence of intrusion events only from the raw audit data, and so the effort required to tune the IDS is reduced.

2.4. *Additional considerations on A-NIDS processing. KDD and data mining*

In addition to the above described A-NIDS techniques, there are others that may help in the task of dealing with the amount of information contained within a dataset. Two of these techniques are *principal component analysis* (PCA) and *association rule discovery*.

PCA is a technique that is used to reduce the complexity of a dataset. It is not a detection scheme itself but an auxiliary one. A given data collection (or dataset), obtained by means of the different sensors in the target environment, becomes more and more extensive and complex as the number of different services and speed of the networks grow. To simplify the dataset, PCA makes a translation on a basis by which n correlated variables are represented in order to reduce the

number of variables to $d < n$, which will be both uncorrelated and linear combinations of the original ones. This makes it possible to express the data in a reduced form, thus facilitating the detection process (Wang and Battiti, 2006).

On the other hand, the aim in association rules discovery is to obtain correlations between different features extracted from the training datasets. By means of these association rules it is possible, for example, to find internal relations between data corresponding to a specific connection. In Cohen (1995) some algorithms for association rules and frequent episodes are contributed.

To conclude the present section, let us present an important discussion of A-NIDS techniques. During recent decades several scientific communities have contributed to analyzing information from high volume databases. However, in the 1990s, KDD (''Knowledge Discovery in Databases'') burst onto the scene, to ''identify new, valid, potentially useful and comprehensible patterns for data'' (Fayyad et al., 1996). *Data mining* techniques appeared as a particular case of KDD (Lee and Stolfo, 1998); these consisted of ''learning algorithms to large data repositories with the purpose of automatically discovering useful information''.

As a specific use case, KDD and data mining have been widely applied in the last few years to correlate traffic instances in network related databases. It is now commonplace to categorize and refer to different IDS processing approaches using the term ''data mining'', as a generic wildcard analysis-related concept. In this line, almost every processing scheme (statistical algorithms, neural networks, fuzzy methods, instance-based learning procedures, and so on) is now considered a data mining technique.

3. Available A-NIDS systems

This section describes several reported endeavours in the development and deployment of A-NIDS platforms in real network environments. The analysis is split into two categories: available platforms, commercial or freeware, and research systems. Commercial systems tend to use well-proven techniques, and so they do not usually consider the A-NIDS techniques most recently proposed in the specialized literature. In fact, most of them include a signature-based detection module as the core of the detection platform. On the other hand, research systems are mainly intended to incorporate the most innovative and recent intrusion methodologies, especially when they are under conditions of development and evaluation.

3.1. *A-NIDS platforms*

In recent years, a number of important actions have focused on implementing A-NIDS techniques in real security platforms. Currently available IDS software tools in this line include Snort (www.snort.org), Prelude (www.prelude-ids.org), and N@G (www.ncb.ernet.in/nag).

Although anomaly-based detection techniques are not yet mature, they are beginning to appear in commercial and open source products. Furthermore, in recent years, some pioneering systems and businesses in the A-NIDS field have been acquired by bigger companies, and their products incorporated into more general and integral network security platforms. Some examples of this are BreachGate WebDefend (Breach Security), based upon G-Server (by Gilian Technologies), and Checkpoint IPS-1 (Checkpoint), from NFR Sentivist IPS (NFR Security).

From a historical point of view, one of the best-known anomaly detection projects was the Statistical Packet Anomaly Detection Engine (SPADE), produced by Silicon Defense. SPADE was defined as a plug-in for Snort, and enabled monitored data to be inspected in search of anomalous behaviour events, from the estimation of a score. Another pioneering system was Login Anomaly Detection (LAD), from Psionic Technologies, which learned user login behaviour and raised an intrusion alarm when any strange activity was detected.

Stealthwatch, from Lancope, used flow-based anomaly detection, and characterized and tracked network activities to differentiate between abnormal and normal network behaviour.

More recent systems make use of a distributed architecture for intrusion detection by incorporating agents (or sensors), and a central console to supervise the overall detection process. This is the case of the SecurityFocus DeepSight Threat Management System – now part of DeepNines BBX Intrusion Prevention (see below for a very brief definition of intrusion prevention systems) – which uses a statistical approach to detect potential Internet threats. Data are collected by distributed sensors, which include intrusion detection capabilities. The sensors report current network scans and attacks to the controller, providing a global detection capability.

Apart from the above tools (some of which are no longer available), Table 2 lists several current intrusion detection/prevention platforms that include anomaly-based detection modules. All of them can be deployed in production environments.

A noticeable feature is the generalized use of a principal signature-based detection module, combined with a complementary anomaly-based scheme. This combination of the two types of detection techniques in a ''Hybrid NIDS'' (PMG, 2001) seeks to improve the overall intrusion detection performance of signature-based systems, while avoiding the usual high false positive rate suffered by A-NIDS methods. Indeed, most existing platforms adopt a hybrid philosophy. Just a few systems (Mazu profiler, nPatrol, SPADE, and Prelude) use only anomaly detection.

Most of the platforms in Table 2 perform further analysis on the monitored data, related to audit, tracing and forensic capabilities. Additionally, they may trigger some kind of response to detected attacks, namely an interaction with firewalls, the reset of TCP connections, the use of honeysystems, etc. The inclusion of prevention mechanisms (such as vulnerability analysis), as well as simulated responses, is also considered in some systems. The most used ones (e.g. Cisco Intrusion Prevention, McAfee IntruShield Network Intrusion Prevention, Checkpoint IPS-1) constitute integral network security solutions.

In some of the platforms examined, the detection techniques used are not explained in sufficient detail by the

Table 2 – Network-based IDS platforms with anomaly detection functionalities, according to the manufacturer's information

Name	Manufacturer	Hybrid	Response	Anomaly-related techniques
AirDefense Guard	AirDefense, Inc.	•	•	Context-aware detection, correlation and multi-dimensional detection engines
Barbedwire IDS Softblade	BarbedWire Technologies	•	•	Protocol analysis, pattern matching
BreachGate WebDefend™	Breach security	•		Behaviour-based analysis, statistical analysis, correlation
Bro	Lawrence Berkeley National Laboratory	•	•	Application level semantics, event analysis, pattern matching, protocol analysis
Checkpoint IPS-1	NFR Security	•	•	Confidence indexing
Cisco Intrusion Prevention System	Cisco Systems	•	•	Behaviour analysis, statistical analysis
DeepNines BBX Intrusion Prevention (IPS)	DeepNines Technologies	•		Multi-Method Inspection (MMI), behaviour analysis, protocol analysis, data correlation
EMERALD	SRI	•	•	Rule-based inference, Bayesian inference
FireProof	Radware Ltd.	•		Protocol anomalies
Firestorm NIDS	Gianni Tedesco	•		Protocol anomalies
Mazu Profiler	Mazu Networks, Inc.			Behaviour analysis (heuristics)
ModSecurity	Ivan Ristic	•		Event correlation
Network at Guard (N@G)	C-DAC (formerly National Centre for Software Technology)	•	•	Protocol anomaly detection, statistical analysis
Next Generation Intrusion Detection Expert System (NIDES)	SRI	•		Statistical analysis
Nitro Security IPS	Nitro Security	•		Behaviour analysis
nPatrol	nSecure			Statistical analysis (profiles)
Portus (PAD)	Livermore Software Laboratories, Inc.	•	•	Protocol anomaly detection
Prelude IDS	Yoann Vandoorselaere et al.			Open platform/multiple anomaly-based modules available (3rd party)
SecureNet IDS/IPS	Intrusion Inc.	•	•	Protocol decoding, protocol anomalies
Siren	Penta Security	•	•	Abnormal user behaviour
Snort IDS	Marty Roesch	•		Open platform/multiple anomaly-based modules available (3rd party)
Snort_inline	Rob McMillen	•	•	Open platform/multiple anomaly-based modules available (3rd party)
Sourcefire ETM	Sourcefire Inc.	•	•	Network behaviour analysis
SPADE	Silicon Defense			Statistical analysis
StealthWatch	Lancope	•	•	Network behaviour analysis, ''concern index''
Strata Guard IDS/IPS	StillSecure	•	•	Behaviour analysis, protocol anomalies
Symantec Intrusion Protection	Symantec	•	•	Behaviour-based
TippingPoint Intrusion Prevention System	3COM/TippingPoint Technologies	•		Statistical analysis, profiles
Toplayer Attack Mitigator IPS	Top Layer Networks	•	•	Statistical analysis, profiles

Note: The ''Hybrid'' column indicates hybrid detection, and the ''Response'' column indicates that some kind of response mechanism is also available.

manufacturer. In fact, the information provided is generally poor, and often overblown and overvalued from a functional perspective. The corresponding anomaly detection modules are usually very simple, being based on some kind of statistical analysis for obtaining a behaviour profile. As an example, DeepNines BBX Intrusion Prevention claims to include anomaly detection, but it is only able to detect improper usages of the three way handshake procedure in TCP or unfair (non-symmetric) utilization of UDP.

More advanced platforms include the Protocol Anomaly Detection (PAD) technique, which is based on the detection of anomalies in the use of protocols. This kind of analysis is adopted in BarbedWire IDS, DeepNines BBX, N@G, and Strata Guard. PAD combines specification-based and statistical characterization A-NIDS techniques to model the behaviour of a given protocol. This can be complemented by using additional A-NIDS techniques.

3.2. *A-NIDS research-related environments*

Although some of the above-mentioned A-NIDS platforms are also usable for research purposes, others have been specifically developed for this. Unlike ''commercial'' A-NIDS systems, research oriented environments include more

innovative anomaly detection techniques. This is the case of Bro, from the Lawrence Berkeley National Laboratory, and EMERALD, from SRI. Bro includes semantic analysis at the application layer, while EMERALD considers rule-based discovery and Bayesian networks. Conceived as research platforms, these systems enable the integration of contributed modules performing additional detection techniques. This is also the case of Snort and Prelude, two of the most widely deployed NIDS tools today.

Current research activities in the field of anomaly-based network intrusion detection are plentiful. Table 3 shows some examples of on-going A-NIDS research projects and systems, some of which also appeared in Table 2. Although the list is not complete, it shows a snapshot of current tendencies and techniques.

Regarding the nature of the techniques applied in the detection process, older systems used statistical methods (IDES, PHAD, ALAD) or expert systems (NIDX, ISCA, Computer Watch). More recently, the explored techniques have been diversified, from state-based transition analysis to neural networks, fuzzy logic and even genetic algorithms. At present, most approaches are related to machine learning by Markov models (GIDRE), *N*-grams (Anagram), and others.

Another observed tendency is the consideration of intrusion prevention procedures or IPS (Intrusion Prevention System), that is, *inline* IDS schemes that filter and analyze all the network traffic accessing the target environment. This has two main consequences. On one hand, most projects have a structured architecture in which various detectors can work jointly, typically in a distributed way (e.g. EMERALD, AAFID, GIDRE). On the other hand, as the detectors are now "pluggable" modules, a specialization of their functions and capabilities can be observed. Thus, individual detectors are designed to monitor only a specific protocol or behaviour (e.g. Anagram targets HTTP payloads), and the global detection capabilities of the platform result from combining and correlating the information from different detectors.

4. Open issues and challenges

Intrusion detection techniques are continuously evolving, with the goal of improving the security and protection of networks and computer infrastructures. Despite the promising nature of anomaly-based IDS, as well as its relatively long existence, there still exist several open issues regarding

Table 3 – Anomaly-based NIDS research projects and systems under development

Name	Entity	Techniques/comments
Anagram	Intrusion Detection Systems Lab, Columbia University	Payload modelling through *N*-grams
Autonomous Agents for Intrusion Detection (AAFID)	CERIAS/Purdue University	Open platform/additional anomaly-based modules available. Distributed architecture (agents)
Bro	Lawrence Berkeley National Laboratory	Development platform. Snort-signatures compatible. Application level semantics, event analysis, pattern matching, protocol analysis. Able to execute response scripts.
Data Mining for Network Intrusion Detection	MITRE corporation	Clustering techniques
Dependable Anomaly Detection with Diagnosis (DADDi)	Various partners	Detection by diversification
EMERALD	SRI	Open distributed platform. Rule-based inference. Bayesian inference
Genetic Art For Intrusion Detection (GA-IDS)	Northwestern University	Genetic algorithms for visualizing malicious activities
GIDRE	University of Granada, UPC	Distributed architecture, stochastic modelling, pattern matching
Intelligent Intrusion Detection (IIDS)	Mississippi State University	Fuzzy data mining
Minnesota INtrusion Detection System (MINDS)	University of Minnesota	Statistical analysis, pattern matching, data mining, outlier detection
Network at Guard (N@G)	C-DAC	Development platform. Protocol anomaly detection, statistical analysis
NETSTAT	University of California	
NFIDS	Informatics & Stat. Center, Tehran University	Fuzzy logic, neural networks
Orchids	Ecole Normale Supérieure (ENS) de Cachan	Real-time event analysis and temporal correlation
Prelude IDS	Yoann Vandoorselaere et al.	Open distributed platform
Shadow IDS	The CIDER Project	Old CIDER. Development platform
Snort IDS	Marty Roesch	Open platform/multiple anomaly-based modules available (3rd party)

Some of them are also available for deployment in real scenarios, see Table 2.

these systems. Some of the most significant challenges in the area are:

- Low detection efficiency, especially due to the high false positive rate usually obtained (Axelsson, 2000). This aspect is generally explained as arising from the lack of good studies on the nature of the intrusion events. The problem calls for the exploration and development of new, accurate processing schemes, as well as better structured approaches to modelling network systems.
- Low throughput and high cost, mainly due to the high data rates (Gbps) that characterize current wideband transmission technologies (Kruegel et al., 2002). Some proposals intended to optimize intrusion detection are concerned with grid techniques and distributed detection paradigms.
- The absence of appropriate metrics and assessment methodologies, as well as a general framework for evaluating and comparing alternative IDS techniques (Stolfo and Fan, 2000; Gaffney and Ulvila, 2001). Due to the importance of this issue, it is analyzed in greater depth below.
- Axelsson (1998) reported that most of the IDS systems perform poorly in defending themselves from attacks. Despite that different mechanisms to elude IDS have been described in the literature (Ptacek and Newsham, 2003), more significant efforts should be done to improve intrusion detection technology in this aspect.
- Another relevant issue is the analysis of ciphered data (e.g. in wireless and mobile environments), although this is also a general problem faced by all intrusion detection platforms. Moreover, this problem could be dealt with by simply locating the detection agents at those functional points in the system where data are available in ''plaintext'' format and, for which the corresponding detection analysis can be carried out without special restrictions.

From this discussion, the main conclusion of the section, and thus of the present report, is that a deeper analysis is required of every one of the mentioned aspects and, thus, of alternative proposals in order to address the near future in the field of A-NIDS with confidence.

4.1. *A-NIDS assessment*

As stated in Section 2, one of the main challenges that researchers must face, when trying to implement and validate a new intrusion detection method, is to assess it and compare its performance with that of other available approaches. It is noticeable that this task is not restricted to A-NIDS, but is also applicable to NIDS (and even to IDS in some cases) in general.

The need for test-beds that provide robust and reliable metrics to quantify NIDS has been suggested, for example, by the National Institute for Standards and Technology (NIST) (Mell et al., 2003). Although some authors defend a testing methodology in real environments, most of them, as in Debar et al. (1998), advocate an evaluation procedure in experimental environments. Both approaches have their pros and their cons. An advantage of assessment in real environments is that the traffic is sufficiently realistic; however, this approach is subject to: (a) the risk of potential attacks, and (b) the possible interruption of the system operation due to simulated attacks. On the other hand, the evaluation of NIDS methodologies in experimental environments involves the generation of synthetic traffic as well as background traffic representing legal users, which is far from being a trivial undertaking.

A number of studies have examined the use of the two types of testing methodologies (Athanasiades et al., 2003). This research is summarized in the following contributions to dealing with traffic databases:

- In 1998, DARPA (Defense Advanced Research Project Agency) initiated a programme at the MIT Lincoln Labs with the aim of providing a complete and realistic benchmarking environment for IDS (Puketza et al., 1997).
- The DARPA project was reviewed in 1999, and the resulting 1999 DARPA/Lincoln Laboratory intrusion detection evaluation dataset (IDEVAL) became a widely used benchmarking tool by which synthetic network traffic was generated (Lippmann et al., 2000).
- Additionally, in 2001, DARPA, in collaboration with other institutions, started the LARIAT (Lincoln Adaptable Real-tIme Assurance Test-bed) programme (Rossey et al., 2001). Unfortunately, LARIAT is restricted to US military environments and to some academic organizations under special circumstances.
- Several contributions in the literature have raised questions about the accuracy of the DARPA simulations (McHugh, 2000; Mahoney and Chan, 2003). In this respect, many efforts have been made to obtain new traffic databases. However, all of these proposals quickly became obsolete, as the traffic was out of date compared with that of current networks. Furthermore, the specifications of the corresponding datasets are not described in detail.
- Another key issue about traffic databases is the confidentiality of the data. Some researchers propose anonymity through IP address masquerading (Fan et al., 2004), which has the advantage of real traffic while avoiding the problem of ciphering. This is a good approach, but sometimes the masquerading process is carried out without any consideration of the information kept in each IP address, workload or URI, which could be useful for some NIDS systems. Therefore, it would be good practice to change the IP addresses in such a way that the relations between the real and the faked addresses are univocal. The same applies to other masqueraded information: user-ID, URI, etc. Usually, these basic rules are not obeyed, and the anonymized databases become useless.
- Other network traffic related studies deal with the problem of standardizing the acquisition and use of real traffic for validating NIDS environments. In this respect, we should cite Bermúdez-Edo et al. (2006), which contributes some proposals on a general methodology to acquire and organize traffic datasets, in order to define an evaluation framework to test the performance of anomaly-based NIDS.

The considerable research effort made to date in the field of NIDS assessment is proof of its importance. However, it remains an open issue and a significant challenge.

5. Summary

Albeit briefly, the present paper discusses the foundations of the main A-NIDS technologies, together with their general operational architecture, and provides a classification for them according to the type of processing related to the "behavioural" model for the target system. Another valuable aspect of this study is that it describes, in a concise way, the main features of several currently available IDS systems/platforms. Finally, the most significant open issues regarding A-NIDS are identified, among which that of assessment is given particular emphasis.

The information presented constitutes an important starting point for addressing R&D in the field of IDS. Faster and more effective countermeasures are needed to cope with the ever-growing number of detected attacks.

Acknowledgments

This work was partially supported by the European CELTIC RED project (CP3-011), by the Spanish Ministry of Industry, Tourism, and Commerce, and by the Spanish project TSI2005-08145-C02-02 (70% FEDER funds).

REFERENCES

Anderson D, Lunt TF, Javitz H, Tamaru A, Valdes A. Detecting unusual program behaviour using the statistical component of the next-generation intrusion detection expert system (NIDES). Menlo Park, CA, USA: Computer Science Laboratory, SRI International; 1995. SRIO-CSL-95-06.

Athanasiades N, Abler R, Levine J, Owen H, Riley G. Intrusion detection testing and benchmarking methodologies. In: Proceedings of the 1st IEEE international workshop on information assurance. IEEE Computer Society Press; 2003. p. 63–72.

Axelsson S. Research in intrusion detection systems: a survey. Technical report. Chalmers University of Technology. Goteborg 1998.

Axelsson S. The Base-rate fallacy and its implications for the difficulty of intrusion detection. ACM Transactions on Information and System Security 2000;3:186–205.

Barnett V, Lewis T. Outliers in statistical data. Wiley, ISBN 9780471930945; 1994.

Bermúdez-Edo M., Salazar-Hernández R., Díaz-Verdejo J.E., García-Teodoro P. Proposals on assessment environments for anomaly-based network intrusion detection systems. LNCS 4347; 2006. p. 210–21.

Breunig M., Kriegel H.P., Ng R.T., Sander J. LOF: identifying density-based local outliers. In: Proceedings of the ACM SIGMOD, International Conference on Management of Data; 2000. p. 93–104.

Bridges S.M., Vaughn R.B. Fuzzy data mining and genetic algorithms applied to intrusion detection. In: Proceedings of the National Information Systems Security Conference; 2000. p. 13–31.

Cansian A.M., Moreira E., Carvalho A., Bonifacio J.M. Network intrusion detection using neural networks. In: International Conference on Computational Intelligence and Multimedia Applications (ICCMA'97); 1997. p. 276–80.

Cohen W.W. Fast effective rule induction. In: Proceedings 12th International Conference on Machine Learning; 1995. p. 115–23.

Debar H., Becker M., Siboni, D. A neural network component for an intrusion detection system. In: IEEE Symposium on Research in Computer Security and Privacy; 1992. p. 240–50.

Debar H, Dacier M, Wespi A, Lampart S. An experimentation workbench for intrusion detection systems. Research Report RZ 2998. IBM Reserarch Division, Zurich Research Laboratory; 1998.

Denning DE, Neumann PG. Requirements and model for IDES – a real-time intrusion detection system. Computer Science Laboratory, SRI International; 1985. Technical Report #83F83-01-00.

Denning ED. An intrusion-detection model. IEEE Transactions on Software Engineering 1987;13(2):222–32.

Detecting hackers (analyzing network traffic) by Poisson model measure. Available from: http://www.ensc.sfu.ca/people/grad/pwangf/IPSW_report.pdf.

Dickerson J.E. Fuzzy network profiling for intrusion detection. In: Proceedings of the 19th International Conference of the North American Fuzzy Information Processing Society (NAFIPS); 2000. p. 301–6.

Estévez-Tapiador JM, García-Teodoro P, Díaz-Verdejo JE. Stochastic protocol modeling for anomaly based network intrusion detection. In: Proceedings of IWIA 2003. IEEE Press, ISBN 0-7695-1886-9; 2003. p. 3–12.

Estévez-Tapiador JM, García-Teodoro P, Díaz-Verdejo JE. Anomaly detection methods in wired networks: a survey and taxonomy. Computer Networks 2004;27(16):1569–84.

Estévez-Tapiador J.M., García-Teodoro P., Díaz-Verdejo J.E. Detection of web-based attacks through Markovian protocol parsing. In: Proc. ISCC05; 2005 p. 457–62.

Fan J, Xu J, Ammar MH, Moon SB. Prefix-preserving IP address anonymization: measurement-based security evaluation and a new cryptography-based scheme. Computers Networks 2004;46(2):253–72.

Fayyad U, Piatetsky-Shapiro G, Smyth P. The KDD process for extracting useful knowledge from volumes of data. Communications of the ACM 1996;29(11):27–34.

Fox K., Henning R., Reed J., Simonian, R. A neural network approach towards intrusion detection. In: 13th National Computer Security Conference; 1990. p. 125–34.

Gaffney J, Ulvila J. Evaluation of intrusion detectors: a decision theory approach. IEEE Symposium on Security and Privacy 2001:50–61.

Heckerman D. A tutorial on learning with Bayesian networks. Microsoft Research; 1995. Technical Report MSRTR-95-06.

Kabiri P, Ghorbani AA. Research in intrusion detection and response – a survey. International Journal of Network Security 2005;1(2):84–102.

Kruegel C, Valeur F, Vigna G, Kemmerer R. Statetul intrusion detection for high-speed networks. IEEE Symposium on Security and Privacy 2002:285–94.

Kruegel C., Mutz D., Robertson W., Valeur F. Bayesian event classification for intrusion detection. In: Proceedings of the 19th Annual Computer Security Applications Conference; 2003.

Lazarevic A, Kumar V, Srivastava J. Intrusion detection: a survey, Managing cyber threats: issues, approaches, and challenges. Springer Verlag; 2005. p. 330.

Lee W., Stolfo S.J. Data mining approaches for intrusion detection. In: Proceedings of the 7th USENIX Security Symposium (SECURITY-98); 1998. p. 79–94.

Li W. Using genetic algorithm for network intrusion detection. C. S.G. Department of Energy; 2004. p. 1–8.
Liao Y, Vemuri VR. Use of K-nearest neighbor classifier for intrusion detection. Computers & Security 2002;21: 439–48.
Lippmann R, Haines J, Fried D, Korba J, Das K. Analysis and results of the 1999 DARPA off-line intrusion detection evaluation. Computer Networks 2000;34(4):579–95.
Mahoney M.V., Chan P.K. Learning nonstationary models of normal network traffic for detecting novel attacks. In: Proceedings of the Eighth ACM SIGKDD; 2002. p. 376–85.
Mahoney M., Chan P.K. An analysis of the 1999 DARPA/Lincoln laboratory evaluation data for network anomaly detection. Florida tech. report CS-2003-02; 2003.
McHugh J. The 1998 Lincoln laboratory IDS evaluation. A critique. In: RAID. LNCS, vol. 1907; 2000. p. 145–61.
Mell P, Hu V, Lippman R, Haines J, Zissman M. An overview o issues in testing intrusion detection systems''. NIST Interagency Report NIST IR 7007. Available from: http://csrc.nist.gov/publications/nistir/nistir-7007.pdf; 2003.
PMG. Maximizing the value of network intrusion detection. A corporate white paper from the product management group ofintrusion.com; 2001.
Portnoy L., Eskin E., Stolfo S.J. Intrusion detection with unlabeled data using clustering. In: Proceedings of The ACM Workshop on Data Mining Applied to Security; 2001.
Ptacek T, Newsham T. Insertion, evasion and denial of service: eluding network intrusion detection. Secure Networks 2003.
Puketza N, Zhang K, Chung M, Mukherjee B, Olsson R. A methodology for testing intrusion detection systems. IEEE Software 1997;4(5):43–51.
Ramadas M, Ostermann S, Tjaden B. Detecting anomalous network traffic with self-organizing maps. In: Recent advances in intrusion detection, RAID. Lecture notes in computer science (LNCS), vol. 2820; 2003. p. 36–54.
Rossey L, Rabek J, Cunnigham R, Fried R, Lippmann R, Zissmann R. LARIAT: Lincoln adaptable real-time information assurance test-bed. RAID; 2001.
Sekar R., Gupta A., Frullo J., Shanbhag T., Tiwari A., Yang H., et al. Specification-based anomaly detection: a new approach for detecting network intrusions. In: Proceedings of the Ninth ACM Conference on Computer and Communications Security; 2002. p. 265–74.
Sequeira K., Zaki M. ADMIT: anomaly-based data mining for intrusions. In: Proceedings of the 8th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining; 2002. p. 386–95.
Sobh TS. Wired and wireless intrusion detection system: classifications, good characteristics and state-of-the-art. Computer Standards & Interfaces 2006;28:670–94.
Staniford-Chen S., Tung B., Porrar P., Kahn C., Schnackenberg D., Feiertag R., et al. The common intrusion detection framework-data formats. 1998. Internet draft 'draft-staniford-cidf-data-formats-00.txt'.
Stolfo SJ, Fan W. Cost-based modeling for fraud and intrusion detection: results from the JAM project. DARPA Information Survivability Conference & Exposition 2000:130–44.
Wang W., Battiti R. Identifying intrusions in computer networks with principal component analysis. In: The First International Conference on Availability, Reliability and Security; 2006. p. 270–79. Vienna, Austria.
Ye N, Emran SM, Chen Q, Vilbert S. Multivariate statistical analysis of audit trails for host-based intrusion detection. IEEE Transactions on Computers 2002;51(7).
Yeung DY, Ding Y. Host-based intrusion detection using dynamic and static behavioral models. Pattern Recognition 2003;36(1): 229–43.

Pedro García-Teodoro received his B.Sc. in Physics (Electronics speciality) from the University of Granada, Spain, in 1989. This same year he was granted by ''Fujitsu España'', and during 1990 by ''IBM España''. Since 1989 he is Associate Professor in the Department of Signal Theory, Telematics and Communications of the University of Granada, and member of the ''Research Group on Signal, Telematics and Communications'' of this University. His initial research interest was concerned with speech technologies, in which he developed his Ph.D. Thesis in 1996. From then, his professional profile has derived to the field of computer and network security, specially focused on intrusion detection and denial of service attacks.

Jesús E. Díaz-Verdejo is Associate Professor in the Department of Signal Theory, Telematics and Communications of the University of Granada (Spain). He received his B.Sc. in Physics (Electronics speciality) from the University of Granada in 1989 and has held a Ph.D. grant from Spanish Government. Since 1990 he is Associate Professor at this University. In 1995 he obtained a Ph.D. degree in Physics. His initial research interest was related with speech technologies, especially automatic speech recognition. He is currently working in computer networks, mainly in computer and network security, although he has developed some work in telematics applications and e-learning systems.

Gabriel Maciá-Fernández is an Assistant Professor in the Department of Signal Theory, Telematics and Communications of the University of Granada (Spain). He received a MS in Telecommunications Engineering from the University of Seville, Spain, and got a Ph.D in 2007 from the University of Granada. From 1999 to 2005 he worked as a specialist consultant in 'Vodafone Spain'. His research was initially focused on multicasting technologies but he is currently working on computer and network security, especially in the field of intrusion detection and response systems, denial of service, web security and secure protocols design.

Enrique Vázquez received his M.Sc. and Ph.D. degrees in Telecommunication Engineering from the Technical University of Madrid, Spain, in 1983 and 1987, respectively. Presently, he is a full professor in the Department of Telematic Engineering of the Technical University of Madrid. He has worked in Spanish and European R&D projects on several areas of telecommunications and computer networks, including protocol performance evaluation, traffic engineering, mobile networks, network convergence, and network security.