Network-based Hybrid Intrusion Detection and Honeysystems as Active Reaction Schemes

Pedro García-Teodoro, Jesús E. Díaz-Verdejo, Gabriel Maciá-Fernández, and Leovigildo Sánchez-Casado

Dpt. of Signal Theory, Telematics and Communications - Faculty of Computer Science and Telecommunications
University of Granada – 18071 Granada – Spain

Summary
This paper presents some proposals and contributions in network-based intrusion-related technologies. Two key points are discussed in this line: anomaly-based intrusion detection, and active response mechanisms. The first issue is mainly focused on the consideration of a stochastic approach to model the normal behavior of the network system to be monitored and protected. This anomaly-based detection methodology is combined with a signature-based one, thus resulting in a hybrid detection system, in order to improve the overall detection throughput. On the other hand, a honeysystem-based approach is also introduced to deal with the development of a pro-active response mechanism in the context of intrusion detection technologies. Both of the aspects, detection and reaction, will be studied as functional modules of an integral intrusion platform developed from a current available IDS tool.

Key words:
Intrusion, Attack, Anomaly, IDS, IRS, Honeysystem.

1. Introduction

The increasing dependence of the society on the information and communications technologies (ICT) makes necessary to improve and to promote the confidence of the users in such systems and services. Nevertheless, this is not a trivial fact at all. Among other considerations, the more and more complexity of networks and communication systems is a direct reason for the exponential growth in the number of vulnerabilities of the mentioned environments, as evidenced through the evolution of the reported incidents in the last years by specialized sources; e.g. CERT ("Computer Emergency Response Team"; http://www.cert.org) and FIRST ("Forum of Incident Response and Security Teams"; http://www.first.org). Several works have been developed up today regarding the study and management of security incidents (e.g. IETF RFC 2350 [1]).

The provision of a set of "security services" to guarantee a certain degree of confidence of the users in ICT, requires the existence of some mechanisms and tools to cover one or more of the numerous aspects involved in the term security: confidentiality, authentication, privacy, availability, etc. One of the most widely used security technology for monitoring and managing networks and communication environments is that of "Intrusion Detection Systems", or IDS. Although IDS contribute actively in the robustness of the global security services offered, and in spite of more than two decades of existence of this kind of systems [2] [3], there still are several limitations and potentials improvements (direct and/or complementary) able to be analyzed in order to increase the performance achieved by current IDS'.

Two are the basic classifications accepted for IDS': the first one, according to the source of the information considered for the detection approach; and the second one, depending on the analysis process that supports the detection itself. Regarding the first criterion, an IDS can be either *network-based* or *host-based*. In network-based IDS' or NIDS, the monitored information corresponds to traffic events related to transmission protocols: IP addresses, source and destination ports, and so on. On the other hand, host-based IDS' or HIDS use information mainly of the OS: process identifier (PID), profiles and user permissions, etc.

Beyond the source of the information considered (network *vs.* host), the type of the analysis carried out on it also drives to the acceptance of two kinds of IDS': *signature-based* IDS or S-IDS, and *anomaly-based* IDS or A-IDS. The detection process in S-IDS' (NIDS and HIDS) tries to find some pattern within the monitored information. For that, a signature database corresponding to well-known attacks is previously defined. Opposite to S-IDS', the A-IDS schemes are based on the disposal of a model related with the *normal* (or *abnormal*) "behavior" of the environment to be protected. Thus, A-IDS' will generate, or not (depending on the analysis basis: normality or abnormality, respectively), intrusion alarms when a certain degree of deviation in the observed events with respect to the expected ones by the model is raised [4].

Manuscript received October 5, 2007
Manuscript revised October 20, 2007

Whatever the approximations to develop an IDS are, a main question regarding this kind of technologies exists: What response mechanisms could be adopted when an intrusion alarm is raised? The so-called ”Intrusion Response Systems” or IRS, appear in this line, they receiving the name of IPS ("Intrusion Prevention Systems") when all the events to be analyzed go through the response device (inline configuration) [5]. The expected benefits from using an IRS (or IPS) can be great if we take into account that the practical totality of the intrusion alarms generated by the current IDS technologies consist of mere notifications (via e-mail, for example) to the management staff, who will handle them later manually. Because the increasing capacity of the network and communication systems at present, the control of the potential triggered alarms should be automated to make more effective their processing. Otherwise, the detection schemes will become useless due to the impossibility of processing the observed intrusion events.

In the above context of detection and response to intrusions, the present work tackles the study of automatic pro-active response mechanisms in the area of the anomaly-based network IDS technologies (A-NIDS). The discussion is founded on a key question: What does “intrusion alarm” mean, in an A-IDS environment? In other words, are the terms "anomaly alarm" and "intrusion alarm" equivalents? Strictly speaking, the response is clear: No, they aren’t! In consequence, what kind of response mechanisms should be considered for A-IDS’? The use of *trap systems* ("honeysystems") to redirect and analyze the flow associated to a given "anomalous event" alarm will be discussed in this document.

The rest of the paper is organized as follows. In Section 2, the work developed by the authors in the field of A-NIDS is described. Next, Section 3 presents the current IRS technologies, and some of the most promising lines in the matter. The employment of trap systems as IRS schemes for A-IDS is dealt with in Section 4, while some contributions regarding the real implementation of an integral NIDS+IRS platform are detailed in Section 5. Finally, Section 6 summarizes the principal conclusions of the work as well as some of the most promising future lines.

2. Developments in NIDS

As previously stated, the present work is focused on intrusion detection systems for network environments (NIDS). The choice of one of the types of IDS approaches relies on the consideration of two main aspects: detection rate and cost of the analysis. Under this perspective, signature-based NIDS’ (S-NIDS) cover nowadays the practical totality of the available systems in this field. And this mainly due to: (a) the detection capacity is theoretically of 100 percent, because of the prior knowledge of the attack patterns[1]; and (b) the simplicity of operation on the basis of the comparison between character strings. However, the principal limitation adduced for S-NIDS’ says to their excessive strictness,, since they are unable to detect attack events (even if they only are slight variants of others prior known) not contemplated into the signature databases used.

In opposite to S-NIDS’, A-NIDS’ (anomaly-based NIDS) present as their main property the theoretical capability to detect intrusion events not previously reported and, therefore, unknown. Nevertheless, this "virtue" is a utopia at present; the reason, the nonexistence of an operative approach to obtain a really representative model of the "normal" and/or "anomalous" behavior of the system to be protected. This generally leads to the disposal of excessively generic models, which provokes a high "false alarms" rate (events detected erroneously as intrusions) during the detection process. Such malfunction is clearly undesirably, since its direct consequence would be, among others, an enormous (and unnecessary!) labor of subsequent analysis, with the corresponding waste of resources that this implies.

2.1. Hybrid NIDS

Is from the previous perspective that the authors are working to join and to integrate S-NIDS’ and A-NIDS’. Named *hybrid* NIDS’ (h-NIDS hereafter), and intended to take advantage of the complementary benefits of both types of approaches, the global detection procedure carried out is that shown in Fig. 1. Two consecutive detection stages should be noticed [6]:

1. In a first one, the network traffic captured is analyzed through by an S-NIDS module, thus generating an attack alarm (in the planned form for it) if a known attack pattern is matched.
2. On the other hand, if the traffic is "clean" from the point of view of the S-NIDS, it will be processed in a second step through by an A-NIDS module arranged for this purpose. This second detection stage will allow, if so, to raise an "anomaly" alarm.

Summarizing, h-NIDS’ are mainly characterized by the following three principal features:

[1] It should be noticed that the patterns defined for certain attacks can be sometimes “wrong” or “incomplete”, and so they must be modified later. Meanwhile, during the interim, the detection rate will be less than 100%.

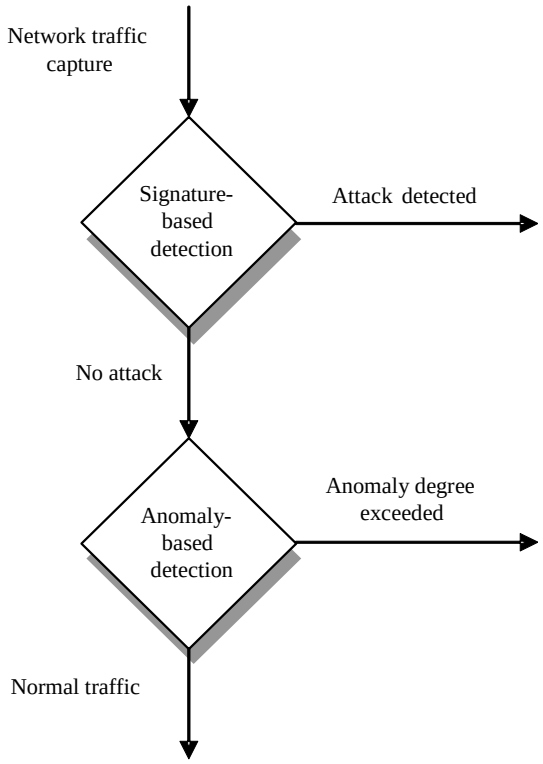

Fig. 1. Combined signature-based and anomaly-based detections in h-NIDS'.

1. Use of known pattern attacks, which implies high computation speed and reliability of the detection process.
2. Theoretical capability for detecting unknown intrusion events.
3. Decrease of the false alarms rate, as a result of a possible less rigid execution of the A-NIDS detection-related process, because of the (previous) signature-based detection stage.

Additionally to the above points, and related with the last one, it is opportune to remember that the false alarms rate depends principally on the throughput of the implemented A-NIDS process. The work developed by the authors in this direction is detailed in the following.

2.2. Contributions to A-NIDS'

As pointed out, the development of anomaly-based NIDS' is a field with important open challenges yet. One of the most relevant is that of the specification of a representative model which collects adequately the real distinguishing features of the analyzed traffic. Thus, the burden of the existing contributions in the specialized literature evidences the excessively generic character of the adopted approach, which indeed provokes a low throughput of the detection process.

The work carried out by the authors in this area is essentially different, taking as initial premises the following two:

– A layered security structure is proposed in the definition of the OSI model, which is analogous to the functional one [7].
– None known traffic event has been reported until now as attack by the simultaneous affectation of more than one network layer.

From this, we propose the development of an A-NIDS approach with the following characteristics [8]:

1. Division of the detection problem into two levels. In the first one, the individualized detection in a layer basis or, more specifically, in a protocol basis (IP, TCP, HTTP, etc) is studied. This approach has been baptized with the acronym LAND, which comes from "LAyered-based Network intrusion Detection". In a second detection level, of optional nature, it is possible to consider a more or less complex correlation analysis among the realized ones for the different individual layers or protocols.
2. The methodology that sustains the individual A-NIDS procedures consists of modeling the normal behavior of every target protocol. Two fundamental aspects have to be taken into account in order to obtain each of the individual models:
   a. Consideration of the formal specifications of the particular protocol.
   b. From them, a stochastic model based on the theory of Markov chains and models is obtained. For this, the considered observations are character strings into the PDU header corresponding to the protocol [9] [10].

In addition to this stochastic methodology, the authors have also proposed two alternative A-NIDS schemes, both of them of geometric nature: one called *N3* [11], and a second one based on *evolutionary algorithms* [12].

The described work about A-NIDS' is essential in the context of the present work, mainly due to the implications of the nature of the alarms handled. The following sections are developed in this line.

3. Response to Intrusions

As it has been exposed, the use of intrusion response mechanisms (IRS) constitutes a relevant fact to improve the security (and its management) in network and communication environments. Diverse requirements to be fulfilled by IRS for a suitable functionality can be found in [13] and [14].

A generic conceptual scheme for an integral detection+response system is shown in Fig. 2. Several functional stages exist. The first phase refers to a *detection* process (IDS), through which the traffic is monitored, filtered and analyzed according to the pursued interests. An *alarm* will be thus triggered in case an intrusion event is observed. This alarm will be *classified* to take the final *decision* about what response to adopt [15] [16]. This phase is the most complex one, since it depends on some factors like severity of the attack, reliability of the information, risk analysis and relevance of the service for the users and the organization. Numerous proposals can be found in this line in the bibliography [17] [18]. Afterwards, the *response* subsystem will act: once the "intrusive event" has been detected, classified and decided the attitude to it, the response mechanism will be run to overcome the circumstance. After generating the response, an *evaluation* phase is intended as a feedback mechanism to study the correspondence response-new_system_state.

Despite the diversity of detection+response approaches currently available, the reality is usually quite different from the ideal aim, there still existing numerous and important the limitations and challenges in the area. Thus, the most of the mechanisms for generating intrusion alarms (independently of the methodology followed by the detection process: signatures *vs*. anomalies, specifications *vs*. stochastic modeling …) relies on the notification (e.g. via e-mail) of such eventuality to the corresponding management staff, which will carry out later a manual actuation. This constitutes a bad response methodology, if not totally useless, due, for example, to the huge volume of traffic existing in current networks [19] [20]. This fact reveals the convenience of adopting automatic response schemes to make possible the actuation, in due time and proper form, against potential intrusion events. This kind of responses also receives the name of *(pro-)active*, to differentiate them from the "passive" ones like those "via e-mail" above indicated. There exist several definitions to the concept of active response or reactions, being one of the most widely accepted that in [21]: *"Actions realized by a process or system against the occurrence of a security incident. Such actions should be oriented to gather information regarding the incident, to limit the users' rights or to block the IP traffic by means of firewalls"*. Despite the aforementioned issues on active responses, it must be bore in mind the critical nature of some of them, especially from a legal perspective.

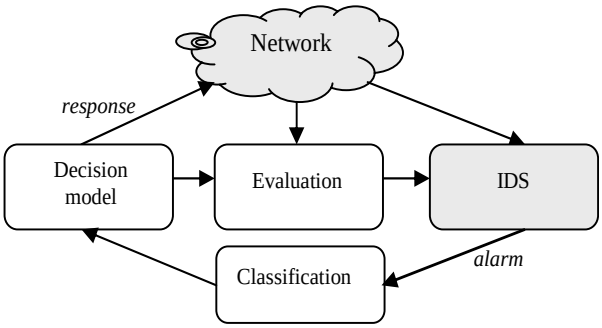

Fig 2. General scheme of an IDS+IRS system.

Very few automatic reaction mechanisms have been proposed in the specialized literature, and even less the actually operative ones. Two of them must be emphasized: modification of firewall rules, and management of access control lists (ACL). Despite the increasing use of both response schemes, especially the first one, it has to be indicated the fact that their implementation neither is always easy nor suitable in the practice. Thus, for example, it is not rare to have a control of the firewall rules isolated in time, disordered in its application and, as a consequence, incoherent as mechanism to guarantee a minimum reliability [22].

Before finishing this section on IRS, it is important to mention an additional issue. Since an A-NIDS generates "anomaly alarms": How to extent, if possible, an IRS oriented to solve well known intrusion events, and accepted as attacks (S-NIDS), to A-NIDS environments? In other words, is it feasible to compare "attack" with "anomaly"? We think that the conversion anomaly-to-attack must go through an analysis stage from which, after studying the implications of the observed event, as well as its characteristics and those of the environment, it could be definitively concluded the malicious nature of the detected activity. A framework is defined in this direction in the following.

4. Honeysystems and IRS'

As established by Spitzner in [23], *honeysystems* constitute an environment specifically designed to attract the attackers' attention, in order to learn methodologies and procedures from malicious actions to strengthen the security of networks and systems. This way, honeysystems are similar tools, somehow, to firewalls, antivirus, IDS, etc., oriented to improve the security of elements and systems in networks and communications. The generic term "honeysystem" covers two variants: *honeynets* and *honeypots*, the first one being a generalization of the second one or, what in fact is the same, the second one a particularization of the first one. *Honeynets* refer to network environments with a variety of software and/or hardware elements, whereas *honeypots* imply the consideration of a single entity (device, service, …).

Honeysystems can be classified according to four criteria [23]:

- Attending to their *installation* and *configuration.* This category measures the time and the effort necessary for starting the system up. The more functionality present, the more complex the installation and operation of the system are.
- According to their *deployment* and *maintenance*. In a similar way to the previous one, the more options and services a honeysystem provides, the more time and resources will be necessary to deploy and maintain the system.
- *Interaction level*. The more interaction between the user and the system is allowed, the more information will be obtained, and, consequently, better the learning is.
- According to the *risk*. High interaction level means more complexity, which causes greater risk. Thus, a honeysystem that allows maximum interactivity to an attacker will be potentially used by this to attack other systems.

4.1. Dynamic honeypots

The first proposal on dynamic honeysystems was introduced by Lance Spitzner in Securityfocus (http://www.securityfocus.com). He established, about a dynamic *honeypot*:

> *"It is automatically determined how many honeypots to deploy, how to deploy them, and what they should look like to blend in with your environment. Even better, the deployed honeypots change and adapt to the environment."*

To configure and implement a dynamic honeysystem is necessary to answer some basic questions related to its learning, deploying, configuration, etc. Spitzner proposes the use of two known technologies to give solution to these questions. One of them is *P0f* (http://lcamtuf.coredump.cx/p0f.shtml), used to protect systems by means of *fingerprinting*. It is possible to know the type of system or application by simply analyzing the network traffic and comparing it with a fingerprints database. This way, we might learn about the network and the employed systems, being able to configure *honeypots* dynamically through the network. An alternative tool to P0f is *Honeyd* (http://www.honeynet.org), which allows creating and deploying *virtual honeysystems*. Honeyd is a low interaction *honeypot*, which simulates just a few parts of the OS (e.g. the network stack).

Dynamic *honeypots* are also dealt with in many other works posterior to that of Spitzner. Thus, the use of a database with information about the machines and the trace files (*logs*) is proposed in [24], with the result that a dynamic honeypot server interacts with the different components of the architecture. In the same line, in [25] different dynamic honeysystems are evaluated. Called *active honeypots* in this case, the authors propose that a honeysystem should react to the attack, as well as to be automatically configured.

4.2. Dynamic honeysystems as IRS schemes in networks

The relevance of dynamic honeysystems lies in two facts: learning and adaptation. Although the second of them, adaptation, is sufficiently clear at this point, that of learning needs to be discussed more in depth.

Learning is a key aspect in the context of IDS+IRS. As it was stated at the end of Section 3, it is necessary to define a procedure to convert an anomaly to an attack. This ought to be an additional phase of the global IDS+IRS system shown in Fig. 2. This new stage, the last one, means the h-NIDS to learn from the analyzed traffic and, in case, to automatically derive a new attack signature, which will be included for its use in the S-NIDS module. Although there are several works aimed to automatically generate signatures for IDS', the use of *honeypots* to do this is only discussed in a few of them [26].

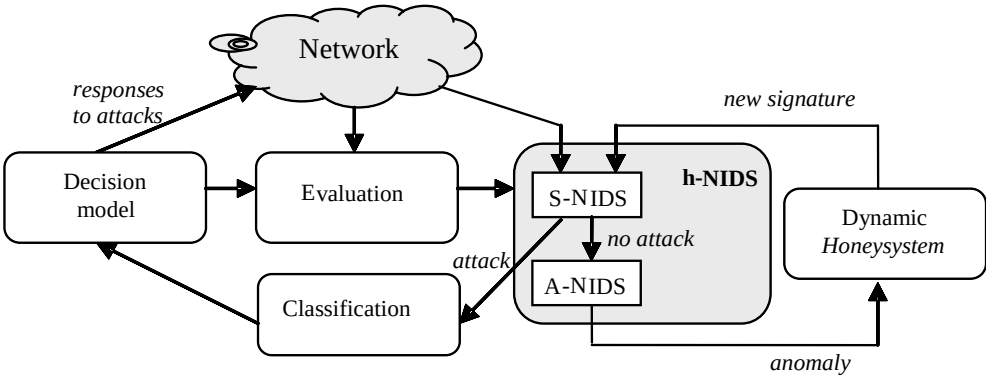

Fig 3. Use of honeysystems as reaction schemes to A-NIDS alarms, in the context of h-NIDS'+IRS'.

A similar approach is carried out by the present work's authors. However, it must be pointed out a clear and crucial difference between both proposals. Opposite to [26], our development is specified from the potential generation of anomaly alarms by a hybrid NIDS system. This insignificant circumstance constitutes a radically different environment from the usual one. In general, honeysystems carry out a (more or less) indiscriminate analysis of the network traffic, while the idea of our proposal is to act only over the traffic/flow/communication for which malicious events are detected, as described in Section 2.2.

The final functional scheme for our h-NIDS+IRS platform is that shown in Fig. 3. Taking Fig. 2 as origin, it is noticeable the incorporation of the learning stage from the detection of anomalies and, from it, at least under a theoretical-conceptual viewpoint, the generation of the hypothetical signature associated, and the pertinent update of the corresponding signature database. For simplicity and without loss of generality, the learning process is specified in an independent way to the S-NIDS module. Although of a different basis, A-NIDS and S-NIDS might be combined into a single global environment. In this case, it would be necessary to take care in defining the functionality of the "Classification", "Decision" and "Evaluation" modules.

As a last conclusion, it is important to signal the complementary nature of the honey-related approach presented here with that given by Kreibich in [26].

5. Proposals for design and implementation

After describing the main work and contributions of the authors in the context of IDS' and IRS', this section will present some notes and proposals regarding the implementation of a real platform to detect and handle intrusion events in network and communication environments, with especial interest in anomalies and, thus, in the development of honeysystems as IRS mechanisms.

Although not many, there exist some developments of honeypots/nets in the context of detection and response to intrusions. For example, in [27] the system *ITS* ("Intrusion Trap System") is contributed, which allows to redirect the communications between an user and a server by means of a non-dynamic honeypot. This, however, is not rigorous in its specifications, neither in the NIDS methodology to use nor in the estimation of the severity of the attacks. On the other hand, the *Collapsar* architecture [28] considers the use of virtual high interaction honeynets to analyze the detected attacks. The virtualization platforms considered for this are *VMware* ("Virtual Machines ware"; http://www.vmware.com) and *UML* ("User-Mode Linux"; http://user-mode-linux.sourceforge.net), both of them with the ability to emulate OS' and different services in a transparent way. Although the traffic analyzed in Collapsar comes from sensors distributed along the target network environment, the considered honeysystems are of static nature.

Some other systems are also available, but all of them are quite similar to the above ones. Regarding the present work, our implementation proposal foresees to sustain the global IDS+IRS platform on Snort (http://www.snort.org), a free distributed and widely adopted NIDS tool. The main features that make Snort attractive are:

– Easy captures of traffic, and wide capability to filter it.

– High availability and updatability of attacks' rule/signature databases.
– Free source, so that users can incorporate new functionalities through pre- and post-processing modules.

From these capacities, and according to that exposed in Sections 2, 3 and 4, we are working on the development and implementation of an NIDS+IRS supported by Snort, and with the following remarkable specific features:

1. Objective of the analysis: HTTP network traffic, in a layer/protocol basis (LAND approach; Section 2.2). No correlation of events among protocols is considered at present.
2. Hybrid NIDS: combined S-NIDS and A-NIDS functionalities, sequentially in time (see Fig. 1). That is to say, the traffic that surpasses all the rules contemplated in Snort (regarding HTTP) will be analyzed by an anomaly detector module, thanks to the definition of an especial ad-hoc rule.
3. A-NIDS methodology: formal protocol specification-based and stochastic modeling of the HTTP service behavior. Although several other approaches have been proved as developed by the authors, the considered one in the specific implementation referred here, is that based on Markov's chains and models (Section 2.2).
4. Response mechanisms: firewall rules and ACL for the S-NIDS functionality, and consideration of dynamic honeypots (having into account the uniqueness of the service, HTTP, approached at this moment) for the A-NIDS method.
5. Learning: the use of dynamic honeypots is additionally foreseen as device for the automatic generation of new attack signatures for the S-NIDS module.

5.1. Preliminary experimental issues

The first three of the five abovementioned objectives are already fully developed and operative in our lab, and their integration into Snort is full and transparent for users. After testing it in (near to) real conditions, the analysis of the system concludes a comparable throughput regarding the detection rate, and superior in some aspects, than the reached one by just considering the exclusive signature-based functionality by Snort. Moreover, it must be also noticed that the additional A-NIDS processing does not consume a significant extra computation time and, thus, a decrease in the overall detection performance.

Opposite to these results, the adoption of active response mechanisms is in an incipient phase yet. Thus, despite the last versions of Snort provide for outputting methods to interact with the *iptables* Linux firewall, this is not currently the case for honey-related tools. In this line, the authors' labor is mainly focused on integrating and evaluating a honeysystem module to collaborate with the h-NIDS+IRS Snort-based platform in a direct way in the protection of the target environment. For that, three main ideas should be mentioned:

– Redirection of the communication corresponding to the detected abnormal packets during the A-NIDS process.
– "Capture" of such flows by means of tools like Honeyd and VMware.
– Some other capture methods are being considered (e.g. deployment of owner honeysystem solutions), so that the analysis of the corresponding results will decide the final choice.

Although the purpose of generating automatically S-NIDS signatures by means of our particular IRS approach is far from being a reality, some interesting preliminary results are available at present in this direction.

6. Conclusions

The present work turns on an integral environment about detection and response to network intrusions. Opposite to other similar tools currently available, there are several remarkable differences with them. First, it is necessary to indicate the consideration of an hybrid detection approach, for which a stochastic normality model is combined with an usual signature-based intrusion detection.

On the other hand, taking into account the particularity of the A-NIDS methodology, the alarms generated will be analyzed with a fine tooth-comb before concluding if they correspond, or not, to attacks. For that, the use of dynamic honeysystems is contemplated, which will make possible the automatic generation of signatures to be incorporated to the S-NIDS module.

Although the implementation for the global platform is not completed, some interesting conclusions can be extracted from its current state. Thus, the authors are convinced in having wider and better versions in the near future.

Acknowledgments

This work has been partially supported by the Spanish Government through MEC (Project TSI2005-08145-C02-02, FEDER funds 70%).

References

[1] RFC 2350: "Expectations for Computer Security Incident Response". IETF ("Internet Engineering Task Force"); http://www.ietf.org/rfc/rfc2350.txt (1998).

[2] J.P. Anderson. "Computer Security Threat Monitoring and Surveillance". Technical report, James P Anderson Co. Fort Washington, Pennsylvania (1980).

[3] E.D. Denning. "An Intrusion-Detection Model". IEEE Transactions on Software Engineering, vol. 13-2, pp. 222-232 (1987).

[4] P. Kabiri, A.A. Ghorbani. "Research in Intrusion Detection and Response – A survey". International Journal of Network Security, vol. 1-2, pp. 84-102 (2005).

[5] M. Rash, A. Orebaugh, G. Clark, B. Pinkard, J. Babbin. *Intrusion Prevention and Active Response*. Syngress Publishing, Inc. (2005).

[6] M. Bermúdez-Edo, R. Salazar-Hernández, J.E. Díaz-Verdejo, P. García-Teodoro. "Proposals on Assessment Environments for Anomaly-based Network Intrusion Detection Systems". Lecture Notes on Computer Science, vol. 4347, pp. 210-221 (2006).

[7] ISO. "Open Systems Interconnection-basic Reference Model Part 2: Security Architecture". International Standards Institute, 7498-2 (1989).

[8] J.M. Estévez-Tapiador. "Detección de Intrusiones en Redes Basada en Anomalías Mediante Técnicas de Modelado de Protocolos". Tesis Doctoral; Dpto. de Teoría de la Señal, Telemática y Comunicaciones. Universidad de Granada (2004).

[9] J.M. Estévez-Tapiador, P. García-Teodoro, J.E. Díaz-Verdejo. "Measuring Normality in HTTP Traffic for Anomaly-based Intrusion Detection". Computer Networks, vol. 5-2, pp. 175-193 (2004).

[10] J.M. Estévez-Tapiador, P. García-Teodoro, J.E. Díaz-Verdejo. "Detection of Web-based Attacks through Markovian Protocol Parsing". 10th IEEE Symposium on Computers and Communications (ISCC), vol. 5-2, pp. 457-462, Cartagena (2005).

[11] J.E. Díaz-Verdejo, J.M. Estévez-Tapiador, P. García-Teodoro. "Aplicación de Técnicas de Agrupamiento a la Detección de Intrusiones en red Mediante N3". I Congreso Nacional de Informática (CEDI) – Simposium sobre Seguridad Informática (S19-SI), pp. 101-108, Granada (2005).

[12] F. Toro-Negro, P. García-Teodoro, J.E. Díaz- Verdejo, G. Maciá-Fernández. "A KNN-based Evolutionary Algorithm for Intrusion Detection in Networks". I Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD), China (2007).

[13] T. Toth, C. Kruegel. " Evaluating the Impact of Automated Intrusion Response Mechanisms". Proceedings of the 18th Annual IEEE Computer Security Applications Conference (2002).

[14] S. Caltagirone, D. Frincke. " The Response Continuum" . Proceedings of the IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 15-17 (2005).

[15] H. Debar, M. Dacier, A. Wespi. " Towards a Taxonomy of Intrusion Detection Systems and Attacks". Computer Networks, vol. 31, pp 805-822 (1999).

[16] M. Papadaki, S.M. Furnell, B.L. Lines, P.L. Reynolds. "A Response-Oriented Taxonomy of IT System Intrusion" . Proceedings of Euromedia, pp. 87-95. Italia (2002).

[17] M. Papadaki, S.M. Furnell, S.J. Lee, B.L. Lines, P.L. Reynolds. " Enhancing Response in Intrusion Detection Systems" . Journal of Information Warfare, vol. 2:1, pp. 90-102 (2002).

[18] S. Caltagirone, D. Frincke. *Adam: Active defense algorihm and model*, in *Aggressive Network Self-Defense*. (N. R. Wyler, Ed.), pp. 287-311, Rockland, MD, USA, Syngress Publishing (2005).

[19] F. Cohen. " Simulating Cyber Attacks, Defenses, and Consequences". IEEE Symposium on Security and Privacy, Special 20th Anniversary Program, Berkeley, CA, (1999).

[20] C.A. Carver Jr.. " Intrusion Response Systems: a Survey". Technical Report, Department of Computer Science, Texas A&M University, College Station (2001).

[21] S.M. Furnell, M. Papadaki, G. Magklaras, A. Alayed. " Security Vulnerabilities and Systems Intrusions – The Need for Automatic Response Frameworks: a Survey". Proceedings of the IFIP 8th Annual Working Conference on Information Security Management & Small Systems Security, USA (2001).

[22] J.G. Alfaro, F. Cuppens, N. Cuppens-Boulahia. "Analysis of Policy Anomalies on Distributed Network Security Setups". 11th European Symposium on Research in Computer Security (ESORICS), LNCS 4189, pp. 496-511. Alemania (2006).

[23] L. Spitzner. *Honeypots Tracking Hackers*. Addison Wesley (2002).

[24] L. Kuwatly, M. Sraj, Z.A. Masri, H. Artail. "A Dynamic Honeypot Design for Intrusion Detection". The IEEE/ACS International Conference on Pervasive Services, ICPS (2004).

[25] D. Joho. "Active Honeypots". Master Thesis, Department of Information Technology. University of Zurich, Suiza (2004).

[26] C. Kreibich, J. Crowcroft. "Honeycomb: Creating Intrusion Detection Signatures using Honeypots". ACM SIGCOMM Computer Communication Review, vol. 34, pp. 51-56 (2004).

[27] K. Takemori, K. Rikitake, Y. Miyake, K. Nakao. "Intrusion Trap System: An Efficient Platform for Gathering Intrusion-related Information". 10th IEEE International Conference on Telecommunications, vol.1, pp. 614-619 (2003).

[28] X. Jiang, D. Xu. “Collapsar: A VM-Based Architecture for Network Attack Detection Center”. Proceedings of the 13th USENIX Security Symposium, San Diego, CA (2004).

Pedro García-Teodoro received the M.S. degree in Physics (Electronics specialty) from the University of Granada (Spain) in 1989. His PhD. was on automatic continuous speech recognition, while his current research interest is focused on network and communications security, especially in intrusion detection and response, DoS attacks, and secure services and protocols.

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. In 1995 he obtained a Ph.D. degree in Physics. His initial research interest was related with speech technologies, especially automatic speech recognition. Currently he is 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 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 the Ph.D in Telecommunications Engineering from the university of Granada. From 1999 till 2005 he worked as a specialist consultant at ‘Vodafone España’, where he was involved in several research projects. His research was initially focused on multicasting technologies but he is currently working on computer and network security, especially in intrusion detection and response systems, and denial of service.

Leovigildo Sánchez-Casado is currently a MS student in Telecommunications Engineering from the University of Granada (Spain) and he has received a research fellowship in the Department of Signal Theory, Telematics and Communications. His research is focused on network security, especially in intrusion detection and response systems.