Visualization of Misuse-based Intrusion Detection: Application to Honeynet Data

Urko Zurutuza [1], Enaitz Ezpeleta[2], Álvaro Herrero [3], and Emilio Corchado[4]

Abstract. This study presents a novel soft computing system that provides network managers with a synthetic and intuitive representation of the situation of the monitored network, in order to reduce the widely known high false-positive rate associated to misuse-based Intrusion Detection Systems (IDSs). The proposed system is based on the use of different projection methods for the visual inspection of honeypot data, and may be seen as a complementary network security tool that sheds light on internal data structures through visual inspection. Furthermore, it is intended to understand the performance of Snort (a well-known misuse-based IDS) through the visualization of attack patterns. Empirical verification and comparison of the proposed projection methods are performed in a real domain where real-life data are defined and analyzed.

Keywords. Projection Models, Artificial Neural Networks, Unsupervised Learning, Soft Computing, Network & Computer Security, Intrusion Detection, Honeypots.

1 Introduction

A network attack or intrusion will inevitably violate one of the three computer security principles -availability, integrity and confidentiality- by exploiting certain vulnerabilities such as Denial of Service, Modification and Destruction [1]. Nowadays, there is a wide range of tools that support the rapid detection and identifica-

[1] Electronics and Computing Department, Mondragon University. Goiru Kalea, 2, 20500 Arrasate-Mondragon, Spain. uzurutuza@mondragon.edu

[2] Electronics and Computing Department, Mondragon University. Goiru Kalea, 2, 20500 Arrasate-Mondragon, Spain. eezpeleta@eps.mondragon.edu

[3] Civil Engineering Department, University of Burgos. C/ Francisco de Vitoria s/n, 09006 Burgos, Spain. ahcosio@ubu.es

[4] Departamento de Informática y Automática, University of Salamanca, Plaza de la Merced s/n, 37008 Salamanca, Spain. escorchado@usal.es

tion of attack attempts and intrusions. The ones applied in this study are briefly introduced in this section.

A honeypot has no authorised function or productive value within the corporate network other than to be explored, attacked or compromised [2]. Thus, a honeypot should not receive any traffic at all. Any connection attempt with a honeypot is then an attack or attempt to compromise the device or services that it is offering-is by default illegitimate traffic. From the security point of view, there is a great deal that may be learnt from a honeypot about a hacker's tools and methods in order to improve the protection of information systems. In a honeynet, all the traffic received by the sensors is suspicious by default. Thus every packet should be considered as an attack or at least as a piece of a multi-step attack.

Snort is a libpcap-based [3] lightweight network intrusion detection system, is one of the most widely deployed IDS. It is a network-based, misuse-based IDS. Snort detects many types of malicious activity in the packet payload that can be characterized in a unique detection signature. It is focused on collecting packets as quickly as possible and processing them in the Snort detection engine.

Misuse-based IDSs entail one main problem; intrusions whose signatures are not archived by the system can not be detected. As a consequence, a misuse-based IDS will never detect a new (previously unseen) attack [4], also known as 0-day attack. The completeness of such IDSs requires regular updating of their knowledge of attacks. Even if the capabilities of Snort allow a deep analysis of the traffic flows, what interests in this research is the detection, alerting and logging of the network packets as they arrive to a Honeynet system.

Visualization is a critical issue in the computer network defence environment, which chiefly serves to generate a synthetic and intuitive representation of the current situation for the network manager; as a result, several research initiatives have recently applied information visualization to this challenging task [5] [6] [7] [8]. Visualization techniques typically aim to make the available statistics supplied by traffic-monitoring systems more understandable in an interactive way. They therefore focus on traffic data as well as on network topology. Regardless of their specific characteristics, these methods all map high-dimensional feature data into a low-dimensional space for presentation purposes. The baseline of the research presented in this study is that soft computing, in general, and unsupervised connectionist models [9, 10], in particular, can prove quite adequate for the purpose of network data visualization through dimensionality reduction. As a result, unsupervised projection models are applied in the present research for the visualization of Honeypot and Snort data. The main associated goal is to analysis and assess the Snort output thanks to visual media.

The remaining sections of this study are structured as follows: section 2 presents the proposed soft computing approach and the neural projection techniques applied in this work. Some experimental results are presented and described in section 3; the conclusions of this study are discussed in section 4, as well as future work.

2 A Visualization based on Soft-Computing

This study proposes the application of projection models for the visualization of honeypot and Snort data. Visualisation techniques have been applied to massive datasets, such as those generated by honeynets, for many years. These techniques are considered a viable approach to information seeking, as humans are able to recognize different features and to detect anomalies by inspecting graphs [11]. The underlying operational assumption of the proposed approach is mainly grounded in the ability to render the high-dimensional traffic data in a consistent yet low-dimensional representation. So, security visualisation tools have to map high-dimensional feature data into a low-dimensional space for presentation. One of the main assumptions of the research presented in this paper is that neural projection models [9, 10], as soft computing techniques, will prove themselves to be satisfactory for the purpose of security data visualisation through dimensionality reduction.

Projection methods can be smart compression tools that map raw, high-dimensional data onto two or three dimensional spaces for subsequent graphical display. By doing so, the structure that is identified through a multivariable dataset may be visually analysed with greater ease.

Visualisation tools can therefore support security tasks in the following way:

- Visualisation tools may be understood intuitively (even by inexperienced staff) and require less configuration time than more conventional tools.
- Providing an intuitive visualization of data allows inexperienced security staff to learn more about standard network behaviour, which is a key issue in ID [12]. The monitoring task can be then assigned to less experienced security staff.

Due to the aforementioned reasons, the present study approaches the analysis of honeynet data from a visualization standpoint. That is, some neural projection techniques are applied for the visualization of such data. The different projection models applied in this study are described in the following sections.

Differentiating from previous studies, Exploratory Projection Pursuit (EPP) [13, 14] models are applied in the present study as a complementary tool for ID analysing real complex high-dimensional honeynet data sets. In this sense, now the output of both the neural model and Snort (the novel applied IDS) are combined for comprehensive analysis and understanding of network status. In keeping with this idea, the Snort output is intuitively visualized comprising some other information inherent in the unsupervised neural visualization. Based on to this visualization, Snort performance may be easily interpreted and analysed, leading to a proper update of its attack patter/rules.

2.1 Principal Component Analysis

Principal Component Analysis (PCA) is a standard statistical technique for compressing data; it can be shown to give the best linear compression of the data in terms of least mean square error. There are several Artificial Neural Networks (ANNs) or connectionist models which have been shown to perform PCA e.g. [15, 16, 17].

This technique describes the variation in a set of multivariate data in terms of a set of uncorrelated variables, in decreasing order of importance, each of which is a linear combination of the original variables. It should be noted that even if we are able to characterize the data with a few variables, it does not follow that an interpretation will ensue.

2.2 Cooperative Maximum Likelihood Hebbian Learning

The Cooperative Maximum Likelihood Hebbian Learning (CMLHL) model [18] extends the Maximum Likelihood Hebbian Learning (MLHL) [14] model, which is based on Exploratory Projection Pursuit (EPP) [13]. Considering an N- dimensional input vector (x), and an M-dimensional output vector (y), with W_{ij} being the weight (linking input j to output i), then CMLHL can be expressed as:

1. Feed-forward step: $y_i = \sum_{j=1}^{\mathbf{N}} W_{ij} x_j, \forall i$ (1)
2. Lateral activation passing: $y_i(t+1) = \left[y_i(t) + \tau(b - Ay) \right]^+$ (2)
3. Feedback step: $e_j = x_j - \sum_{i=1}^{M} W_{ij} y_i, \forall j$ (3)
4. Weight change: $\Delta W_{ij} = \eta . y_i . sign(e_j) | e_j |^{p-1}$ (4)

Where: η is the learning rate, τ is the "strength" of the lateral connections, b the bias parameter, p a parameter related to the energy function [14, 18] and A a symmetric matrix used to modify the response to the data [18]. The effect of this matrix is based on the relation between the distances separating the output neurons.

3 Analyzing Real-life Data from a Honeynet

The Euskalert project [13] has deployed a network of honeypots in the Basque Country (northern Spain) where eight companies and institutions have installed one of the project's sensors behind the firewalls of their corporate networks. The honeypot sensor transmits all the traffic received to a database via a secure communication channel.

This honeypot system receives 4000 packets a month on average. All the traffic is analyzed by the Snort IDS, and an alert is launched whenever the packet matches a known attack signature. Each incoming packet is inspected and compared with the default rule base. This way, many of them match the Snort rule base signatures. Thereby, even if a big amount of packets cause more than one alarm to be triggered, it facilitates a simple way to separate the alarm set into two subsets:

- Alarms that have been triggered when matching the Snort default rule base. This dataset can be considered as known attack data.
- Alarms that did not match any of the known attack rules. Considered as the unknown data and related to attacks as all the traffic targeting Euskalert.

These two subsets allow further research to distinguish between the known and unknown attack traffic. This permits testing the success rate of Snort, and also visualizing the unknown traffic looking for new and unknown attacks. In some sense, Snort is used as a network data classifier, without discarding any packet. In addition to the default rules of the Snort community, three basic rules that log all TCP, UDP and ICMP traffic have been applied.

The experimental research has been done by using data related to one month of real attacks that reached the 8 sensors used by the Euskalert project [13]. These data are depicted through different neural projections in order to discover real attack behaviour and strategies. For this experiment, we have analysed the logs coming from Euskalert and Snort gathered during February 2010.

The February 2010 dataset contains a total of 3798 packets, including TCP, UDP and ICMP traffic received by the distributed honeypot sensors.

From this dataset, it may be said that Snort is only capable of identifying about 10.38% of bad-intentioned traffic. Furthermore, it was demonstrated that only 2% of the unsolicited traffic was identified by the IDS when automatically generated signatures were included from a previous work [19]. Thus, a deeper analysis of the data is needed in order to discover the internal structure of the remaining close to 90% of the traffic. Explaining the behaviour of the unknown traffic is a difficult task that must be performed to better protect and understand computer networks and systems.

3.2 Experimental Results

The following features were extracted from each one of the records in the dataset:

- **Time**: the time when the attack was detected. Difference in relation to the first attack in the dataset (in minutes).
- **Protocol**: whether TCP, UDP or ICMP (codified as three binary features).
- **Ip_len**: number of bytes in the packet.
- **Source Port**: number of the port from which the source host sent the packet. In ICMP protocol, this represents the ICMP type field.
- **Destination Port**: destination host port number to which the packet is sent. In the ICMP protocol, this represents the ICMP type field.
- **Flags**: control bits of a TCP packet, which contains 8 1-bit values.
- **Snort output**: binary feature stating whether the record triggered a Snort alarm or not.

The previously introduced projection techniques were applied to this real dataset, generating the projections shown in this section. In these projections, the data are depicted with different colors and shapes, taking into account the Snort output:

- **Black crosses**: meaning that the packets triggered any of Snort rules.
- **Red circles**: meaning that the packets did not trigger any of Snort rules.

Fig. 1 shows the CMLHL projection by considering the Snort output. This was selected as the best visualization offered by the different applied projection models. The visualizations obtained from other models are gathered and shown in next sub-section 3.3.

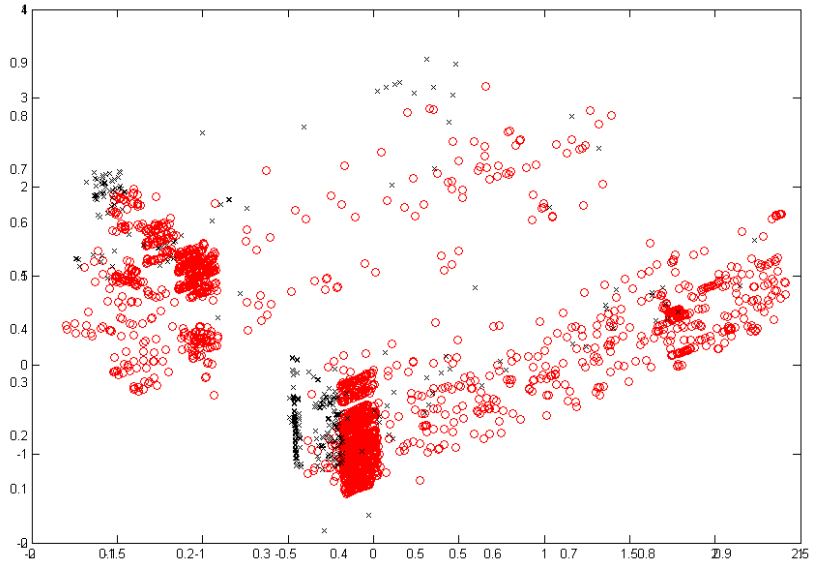


Fig. 1. CMLHL projection – Snort output**.**

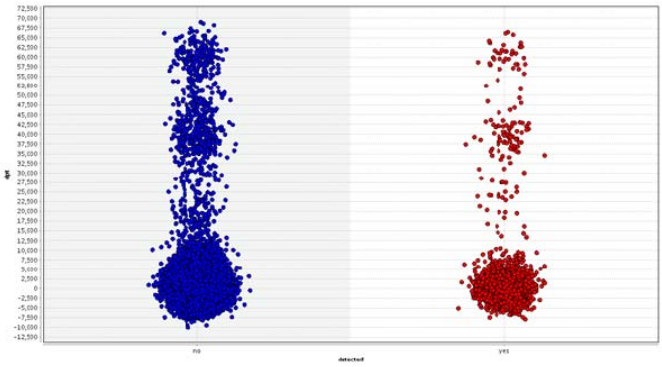
From this visualization, it can be concluded that most of the traffic corresponds to unknown packets, were Snort did not provide any explanation or alert for the

suspicious packets received. Snort can only detect attacks on well-known services. A deeper analysis on what is detected and what is not, arise the fact that most of ICMP traffic (probes and error codes) and a big amount of traffic targeting privileged destination ports is detected.

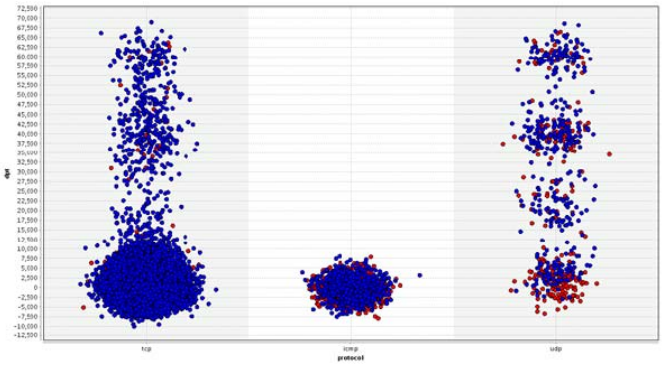
3.3 Comparative Study

For comparative purposes, some other visualizations of the Euskalert-Snort data were generated. Firstly, scatter plot visualizations of the original features of the data were obtained, the best of them selected and included in this study (Figs. 3 and 4). In these visualizations, the data are depicted with different colors, taking into account the Snort output:

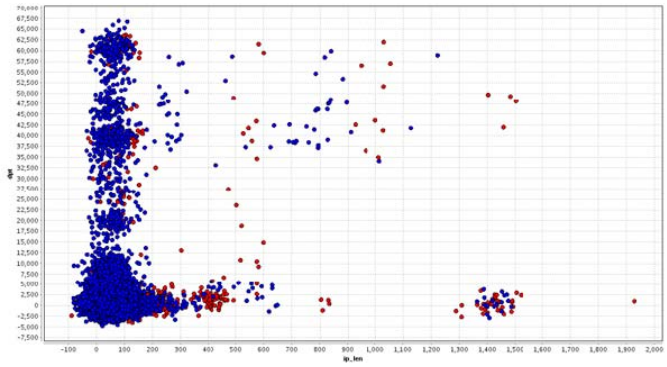
- **Blue**: meaning that the packets did not trigger any of Snort rules.
- **Red**: meaning that the packets triggered any of Snort rules.



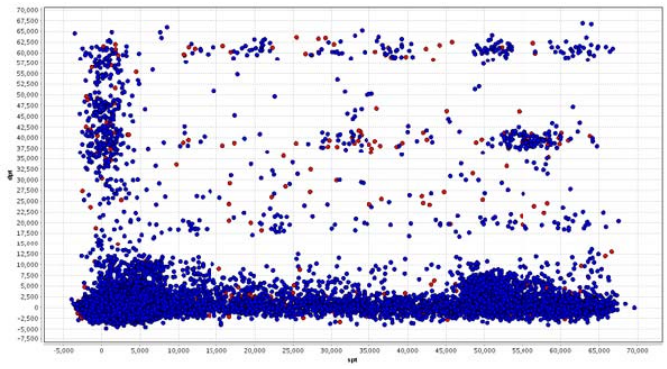
a) Destination port



b) Destination port & Protocol



c) Destination port & IP length



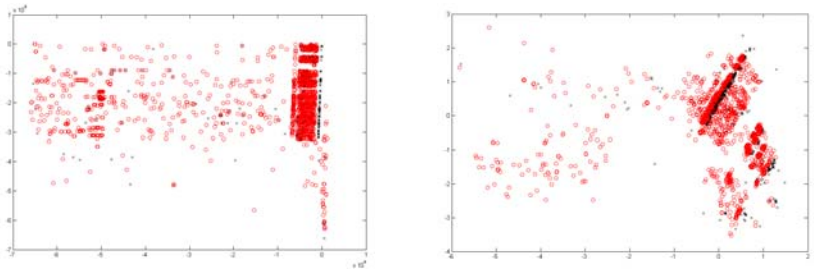
d) Destination port & Source port

Fig. 2**.** Visualizations based on the original features of the data and the Snort output.

It can be said, after analysing these visualizations that scatter plots provide with basic information of the discovered attacks. The first visualization (Fig. 2.a) shows that most of the detected packets target low port numbers (non-privileged). The main reason for such happening is that Snort signatures are created for known attacks exploiting widely used vulnerable applications. Figure 2.b. is not very clear one, but shows that UDP and ICMP traffic have more undetected traffic than TCP. How the destination port is distributed among the different protocols is also an interesting outcome of this visualization (for ICMP, its type is coded into destination port). An analysis of the graphical representation of data according to packet length and destination port (Fig. 2.c) shows more red or undetected phenomena for bigger packets. These are specially created packets for DoS or buffer overflows, but it seems it is not trivial for Snort signature creators to develop these types of

rules. However, red points in the bottom-left side show that some of them already exist. Finally, figure 2.d. shows a very messy representation when matching source and destination ports. The bottom horizontal line is a normal situation, where attacks against known applications are carried out using source ports bigger than 1023, but it can also be found a vertical line representing backscatter phenomena, where packets received are responses from attacked machines from spoofed addresses.

These conclusions are taken from elemental scatter plots and required an advanced security knowledge. For a comprehensive comparison, some projection techniques, namely PCA (see section 2.1) and MLHL, were applied to the data under study. The obtained projections are shown in Fig. 3.



a) PCA projection b) MLHL projection

Fig. 3**.** Projections of data captured by Euskalert (February, 2010) according to Snort output.

In both visualizations known and unknown data is clearly identified and shown. PCA identifies most of the detected attacks related to protocol. Black dots in the left vertical line represent matching signatures, but also ICMP related events. The same can be observed for the MLHL projection, but getting a bit more scatter and structured projection.

4 Conclusions and Future Research Lines

From the projections in Figs. 1 and 2 we can conclude that CMLHL provides a more sparse representation than the other two methods (PCA and MLHL). This enables the intuitive visualization of the honeynet and Snort data.

Thanks to the CMLHL projections it is easy to get a general idea of the dataset structure and Snort performance, and an in-deep analysis can be subsequently carried out. From the analysed dataset, CMLHL gives a more clear representation and allows distinction between the detected traffic and those packets that are not.

Future work will combine some other soft-computing techniques for the intuitive visualization of Honeynet and Snort data.

Acknowledgments. This research has been partially supported through the Regional Government of Gipuzkoa, the Department of Research, Education and Universities of the Basque Government; and the Spanish Ministry of Science and Innovation (MICINN) under project CIT-020000-2009-12 (funded by the European Regional Development Fund); project of the Spanish Ministry of Science and Innovation TIN2010-21272-C02-01 (funded by the European Regional Development Fund). The authors would also like to thank the vehicle interior manufacturer, Grupo Antolin Ingenieria S.A., within the framework of the MAGNO2008 - 1028.- CENIT Project also funded by the MICINN.

References

1. Myerson, J.M. (2002) Identifying Enterprise Network Vulnerabilities. International Journal of Network Management 12(3): 135-144
2. Charles, K.A. (2004) Decoy Systems: A New Player in Network Security and Computer Incident Response. International Journal of Digital Evidence 2(3)
3. libpcap. http://www-nrg.ee.lbl.gov/
4. Rizza, J.M. (2005) Computer Network Security. Springer US
5. D'Amico, A.D., Goodall, J.R., Tesone, D.R., Kopylec, J.K. (2007) Visual Discovery in Computer Network Defense. IEEE Computer Graphics and Applications 27(5): 20-27
6. Goodall, J.R., Lutters, W.G., Rheingans, P., Komlodi, A. (2006) Focusing on Context in Network Traffic Analysis. IEEE Computer Graphics and Applications 26(2): 72-80
7. Itoh, T., Takakura, H., Sawada, A., Koyamada, K. (2006) Hierarchical Visualization of Network Intrusion Detection Data. IEEE Computer Graphics and Applications 26(2): 40-47
8. Livnat, Y., Agutter, J., Moon, S., Erbacher, R.F., Foresti, S. (2005) A Visualization Paradigm for Network Intrusion Detection. (ed) Sixth Annual IEEE SMC Information Assurance Workshop, 2005. IAW '05.
9. Herrero, Á., Corchado, E., Gastaldo, P., Zunino, R. (2009) Neural Projection Techniques for the Visual Inspection of Network Traffic. Neurocomputing 72(16-18): 3649-3658
10. Herrero, Á., Corchado, E., Pellicer, M.A., Abraham, A. (2009) MOVIH-IDS: A Mobile-Visualization Hybrid Intrusion Detection System. Neurocomputing 72(13-15): 2775-2784
11. Ahlberg, C., Shneiderman, B. (1999) Visual Information Seeking: Tight Coupling of Dynamic Query Filters with Starfield Displays. (ed) Readings in Information Visualization: using Vision to Think. Morgan Kaufmann Publishers Inc. 244-250
12. Goodall, J.R., Lutters, W.G., Rheingans, P., Komlodi, A. (2005) Preserving the Big Picture: Visual Network Traffic Analysis with TNV. (ed) IEEE Workshop on Visualization for Computer Security (VizSEC 05). IEEE Computer Society.
13. Friedman, J.H., Tukey, J.W. (1974) A Projection Pursuit Algorithm for Exploratory Data-Analysis. IEEE Transactions on Computers 23(9): 881-890
14. Corchado, E., MacDonald, D., Fyfe, C. (2004) Maximum and Minimum Likelihood Hebbian Learning for Exploratory Projection Pursuit. Data Mining and Knowledge Discovery 8(3): 203-225
15. Oja, E. (1982) A Simplified Neuron Model as a Principal Component Analyzer. Journal of Mathematical Biology 15(3): 267-273
16. Sanger, D. (1989) Contribution Analysis: a Technique for Assigning Responsibilities to Hidden Units in Connectionist Networks. Connection Science 1(2): 115-138
17. Fyfe, C. (1997) A Neural Network for PCA and Beyond. Neural Processing Letters 6(1-2): 33-41

18. Corchado, E., Fyfe, C. (2003) Connectionist Techniques for the Identification and Suppression of Interfering Underlying Factors. International Journal of Pattern Recognition and Artificial Intelligence 17(8): 1447-1466
19. Zurutuza, U., Uribeetxeberria, R., Zamboni, D. (2008) A Data Mining Approach for Analysis of Worm Activity through Automatic Signature Generation. (ed) 1st ACM Workshop on AISec. ACM.