International Journal of Advanced Research in IT and Engineering

ISSN: 2278-6244

AUTONOMOUS NETWORK SECURITY FOR DETECTION OF NETWORK ATTACKS

Nita V. Jaiswal*

Prof. D. M. Dakhne**

Abstract: *Current network monitoring systems rely strongly on signature-based and supervised-learning-based detection methods to hunt out network attacks and anomalies. The unsupervised detection of network attacks represents an extremely challenging goal. In this paper we present a completely unsupervised approach to detect attacks, without relying on signatures, labeled traffic, or training. The method uses robust clustering techniques to detect anomalous traffic flows, sequentially captured in a temporal sliding-window basis.*

The structure of the anomaly identified by the clustering algorithms is used to automatically construct specific filtering rules that characterize its nature, providing easy-to-interpret information to the network operator. The clustering algorithms are highly adapted for parallel computation, which permits to perform the unsupervised detection and construction of signatures in an online basis. We evaluate the performance of this new approach to discover and to build signatures for different network attacks without any previous knowledge, using real traffic traces. Results show that knowledge-independent detection and characterization of network attacks is possible, opening the door to a whole new generation of autonomous security algorithms.

Index Terms—*Unsupervised Anomaly Detection & Characterization, Robust & Distributed Clustering, Automatic Generation of Signatures, Autonomous Security.*

INTRODUCTION

Network traffic anomaly detection has become a vital network building-block for any ISP in today's Internet. Ranging from non-malicious unexpected events such as flash-crowds and failures, to network attacks such as Denials-of-Service (DoS/DDoS), network scans, and spreading worms, network traffic anomalies can have serious detrimental effects on the performance and integrity of the network. The principal challenge in automatically detecting and analyzing traffic anomalies is that these are a moving target. It is virtually impossible to precisely define the set of anomalies that may arise, especially in the case of network attacks, because new attacks as well a new variant of already known attacks are continuously emerging. A general anomaly detection system should therefore be able to detect a wide range of anomalies with diverse structure, using the least amount of previous information, ideally no information at all.

The principal challenge in automatically detecting and analyzing network attacks is that these are a moving and ever-growing target [1]. Two different approaches are by far dominant in the literature and commercial security devices: signature-based detection and anomaly detection. Signature-based detection systems are highly effective to detect those attacks which they are programmed to alert on. However, they cannot defend the network against unknown attacks. Even more, building new signatures is expensive and time-consuming, as it involves manual inspection by human experts. Anomaly detection uses labeled data to build normal-operation-traffic profiles, detecting anomalies as activities that deviate from this baseline. Such methods can detect new kinds of network attacks not seen before. In this paper we present a completely unsupervised method to detect and characterize network attacks, without relying on signatures, training, or labeled traffic of any kind. Our approach relies on robust clustering algorithms to detect both well-known as well as completely unknown attacks, and to automatically produce easy-to-interpret signatures to characterize them, both in an on-line basis.

BODY

A general anomaly detection system should therefore be able to detect a wide range of anomalies with diverse structure, using the least amount of previous information, ideally no information at all.

Two different approaches are by far dominant in current research literature and commercial detection systems: signature-based detection and anomaly detection. Signature-based detection is the de-facto approach used in standard security devices such as IDSs, IPSs, and firewalls. When an attack is discovered, generally after its occurrence during a diagnosis phase, the associated anomalous traffic pattern is coded as a signature by human experts, which is then used to detect a new occurrence of the same attack. Signature-based detection methods are highly effective to detect those attacks which they are programmed to alert on. However, they cannot defend the network against new attacks, simply because they cannot recognize what they do not know. In addition, building new signatures is a resources-consuming task, as it involves manual traffic inspection by human experts.

On the other hand, anomaly detection uses labeled data to build normal operation-traffic profiles, detecting anomalies as activities that deviate from this baseline. Such methods can detect new kinds of network attacks not seen before. Nevertheless, anomaly detection requires training for profiling, which is time consuming and depends on the availability of purely anomaly-free traffic data-sets. Labeling traffic as anomaly-free is not only time consuming and expensive, but also prone to errors in the practice, since it is difficult to guarantee that no anomalies are buried inside the collected data. In addition, it is not easy to keep an accurate and up-to-date normal-operation profile.

The problem of network anomaly detection has been extensively studied during the last decade. Most of the approaches analyze statistical variations of traffic volume descriptors (e.g., number of packets, bytes, or new flows) and/or particular traffic features (e.g., distribution of IP addresses and ports), using either single-link measurements or network-wide data. A non-exhaustive list of standard methods includes the use of signal processing techniques (e.g., ARIMA modeling, wavelets-based filtering) on single-link traffic measurements [2,3],Kalman filters [4] for network-wide anomaly detection, and Sketches applied to IP-flows [6–8].

Our approach falls within the unsupervised anomaly detection domain. The vast majority of the unsupervised detection schemes proposed in the literature are based on clustering and outliers detection, being [11–13] some relevant examples. In [11], authors use a single-linkage hierarchical clustering method to cluster data from the KDD'99 data-set, based on the standard Euclidean distance for inter-patterns similarity. [12] reports improved results in

the same data-set, using three different clustering algorithms: Fixed-Width clustering, an optimized version of k-NN, and one class SVM. [13] presents a combined density-grid-based clustering algorithm to improve computational complexity, obtaining similar detection results. PCA and the sub-space approach is another well-known unsupervised anomaly detection technique, used in [5,7] to detect network-wide traffic anomalies in highly aggregated traffic flows.

Our paper is that these two knowledge-based approaches are not sufficient to tackle the anomaly detection problem, and that a holistic solution should also include knowledge-independent analysis techniques. To this aim we propose UNADA, an Unsupervised Network Anomaly Detection Algorithm that detects network traffic anomalies without relying on signatures, training, or labeled traffic of any kind.

REFERENCES

[1] S. Hansman, R. Hunt "A Taxonomy of Network and Computer Attacks", in *Computers and Security*, vol. 24 (1), pp. 31-43, 2005.

[2]. P. Barford, J. Kline, D. Plonka, and A. Ron, "A Signal Analysis of Network Traffic Anomalies", in Proc. ACM IMW, 2002.

[3]. J. Brutlag, "Aberrant Behavior Detection in Time Series for Network Monitoring", in Proc. 14th Systems Administration Conference, 2000.

[4]. A. Soule et al., "Combining Filtering and Statistical Methods for Anomaly Detection", in in Proc. ACM IMC, 2005.

[5]. A. Lakhina, M. Crovella, and C. Diot, "Diagnosing Network-Wide Traffic Anomalies", in Proc. ACM SIGCOMM, 2004

[6]. B. Krishnamurthy et al., "Sketch-based Change Detection: Methods, Evaluation, and Applications", in Proc. ACM IMC, 2003.

[7]. A. Lakhina, M. Crovella and C. Diot, "Mining

[8]. G. Dewaele et al., "Extracting Hidden Anomalies using Sketch and non Gaussian Multi-resolution Statistical Detection Procedures", in Proc. SIGCOMM LSAD,2007.

[9] A. Lakhina, M. Crovella, C. Diot, "Mining Anomalies Using Traffic Feature Distributions", in *Proc. ACM SIGCOMM*, 2005.

[10] A. Lakhina, M. Crovella, C. Diot, "Diagnosing Network-Wide Traffic Anomalies",in *Proc. ACM SIGCOMM*, 2004.

[11]. L. Portnoy, E. Eskin, and S. Stolfo, "Intrusion Detection with Unlabeled Data Using Clustering", in Proc. ACM DMSA Workshop, 2001.

[12]. E. Eskin et al., "A Geometric Framework for Unsupervised Anomaly Detection: Detecting Intrusions in Unlabeled Data", in Applications of Data Mining in Computer Security, Kluwer Publisher, 2002.

[13]. K. Leung and C. Leckie, "Unsupervised Anomaly Detection in Network Intrusion Detection Using Clustering", in Proc. ACSC05, 2005.