Title: An Information-Theoretic Method for the Detection of Anomalies in Network Traffic

Author: Christian Callegari, Stefano Giordano, Michele Pagano

PII: S0167-4048(17)30143-8
DOI: http://dx.doi.org/doi: 10.1016/j.cose.2017.07.004
Reference: COSE 1170

To appear in: *Computers & Security*

Received date: 14-2-2017
Revised date: 6-6-2017
Accepted date: 5-7-2017

Please cite this article as: Christian Callegari, Stefano Giordano, Michele Pagano, An Information-Theoretic Method for the Detection of Anomalies in Network Traffic, *Computers & Security* (2017), http://dx.doi.org/doi: 10.1016/j.cose.2017.07.004.

An Information-Theoretic Method for the Detection of Anomalies in Network Traffic

Christian Callegari[†‡], Stefano Giordano[†], and Michele Pagano[†]

[†]Dept. of Information Engineering, University of Pisa, Italy

[‡]RaSS National Laboratory – CNIT, Pisa, Italy

E-mail:{c.callegari, s.giordano, m.pagano}@iet.unipi.it

***Abstract*—Anomaly-based Intrusion Detection is a key research topic in network security due to its ability to face unknown attacks and new security threats. For this reason, many works on the topic have been proposed in the last decade. Nonetheless, an ultimate solution, able to provide a high detection rate with an acceptable false alarm rate, has still to be identified.**

In this paper we propose a novel intrusion detection system that performs anomaly detection by studying the variation in the entropy associated to the network traffic. To this aim, the traffic is first aggregated by means of random data structures (namely three-dimension reversible sketches) and then the entropy of different traffic descriptors is computed by using several definitions.

The experimental results obtained over the MAWILab dataset validate the system and demonstrate the effectiveness of our proposal for a proper set of entropy definitions.

***Index Terms*—Anomaly Detection, Information Theory, Shannon Entropy, Tsallis Entropy, Rényi Entropy, Kullback-Leibler Divergence, Jensen-Shannon Divergence, MAWILab**