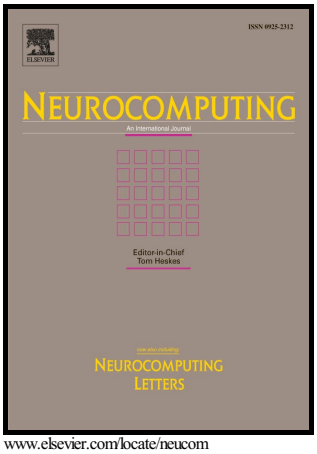
A two-level hybrid approach for intrusion detection

Chun Guo, Yuan Ping, Nian Liu, Shou-Shan Luo



www.elsevier.com/locate/neucom

PII: S0925-2312(16)30659-2
DOI: http://dx.doi.org/10.1016/j.neucom.2016.06.021
Reference: NEUCOM17271

To appear in: *Neurocomputing*

Received date: 12 February 2016
Revised date: 6 June 2016
Accepted date: 9 June 2016

Cite this article as: Chun Guo, Yuan Ping, Nian Liu and Shou-Shan Luo, A two-level hybrid approach for intrusion detection, *Neurocomputing* http://dx.doi.org/10.1016/j.neucom.2016.06.021

A two-level hybrid approach for intrusion detection

Chun Guo[a,b,*], Yuan Ping[c,*], Nian Liu[d], Shou-Shan Luo[b]

[a] *College of Computer Science and Technology, GuiZhou University, GuiYang, 550025, China*

[b] *Information Security Centre, Beijing University of Posts and Telecommunications, P.O Box 145, Beijing, 100876, China*

[c] *School of Information Engineering, Xuchang University, Xuchang, 461000, China*

[d] *Beijing Electronic Science and Technology Institute, Beijing, 100070, China*

Abstract

To exploit the strengths of misuse detection and anomaly detection, an intensive focus on intrusion detection combines the two. From a novel perspective, in this paper, we proposed a hybrid approach toward achieving a high detection rate with a low false positive rate. The approach is a two-level hybrid solution consisting of two anomaly detection components and a misuse detection component. In stage 1, an anomaly detection method with low computing complexity is developed and employed to build the detection component. The k-nearest neighbors algorithm becomes crucial in building the two detection components for stage 2. In this hybrid approach, all of the detection components are well-coordinated. The detection component of stage 1 becomes involved in the course of building the two detection components of stage 2 that reduce the false positives and false negatives generated by the detection component of stage 1. Experimental results on the KDD'99 dataset and the Kyoto University Benchmark dataset confirm that the proposed hybrid approach can effectively detect network anomalies with a low false positive rate.

Keywords: Intrusion detection, Hybrid approach, Anomaly detection, k-nearest neighbors algorithm

*Corresponding author.

E-mail addresses:gc_gzedu@163.com(C.Guo),pingyuan@bupt.edu.cn(Y.Ping), pidstuliu@163.com(N.Liu),luoshoushan@safe-code.com(SS.Luo)