World Academy of Science, Engineering and Technology
International Journal of Electrical and Information Engineering
Vol:10, No:03, 2016

Using Vulnerability to Reduce False Positive Rate in Intrusion Detection Systems

Authors : Nadjah Chergui, Narhimene Boustia

Abstract : Intrusion Detection Systems are an essential tool for network security infrastructure. However, IDSs have a serious problem which is the generating of massive number of alerts, most of them are false positive ones which can hide true alerts and make the analyst confused to analyze the right alerts for report the true attacks. The purpose behind this paper is to present a formalism model to perform correlation engine by the reduction of false positive alerts basing on vulnerability contextual information. For that, we propose a formalism model based on non-monotonic JClassicδε description logic augmented with a default (δ) and an exception (ε) operator that allows a dynamic inference according to contextual information.

Keywords : context, default, exception, vulnerability
Conference Title : ICISS 2016 : International Conference on Information Systems Security
Conference Location : Madrid, Spain
Conference Dates : March 24-25, 2016