World Academy of Science, Engineering and Technology
International Journal of
Vol:8, No:, 2014

e-Learning Security: A Distributed Incident Response Generator

Authors : Bel G Raggad

Abstract : An e-Learning setting is a distributed computing environment where information resources can be connected to any public network. Public networks are very unsecure which can compromise the reliability of an e-Learning environment. This study is only concerned with the intrusion detection aspect of e-Learning security and how incident responses are planned. The literature reported great advances in intrusion detection system (ids) but neglected to study an important ids weakness: suspected events are detected but an intrusion is not determined because it is not defined in ids databases. We propose an incident response generator (DIRG) that produces incident responses when the working ids system suspects an event that does not correspond to a known intrusion. Data involved in intrusion detection when ample uncertainty is present is often not suitable to formal statistical models including Bayesian. We instead adopt Dempster and Shafer theory to process intrusion data for the unknown event. The DIRG engine transforms data into a belief structure using incident scenarios deduced by the security administrator. Belief values associated with various incident scenarios are then derived and evaluated to choose the most appropriate scenario for which an automatic incident response is generated. This article provides a numerical example demonstrating the working of the DIRG system.

Keywords : decision support system, distributed computing, e-Learning security, incident response, intrusion detection, security risk, statefull inspection