A cost-sensitive entropy-based network security situation assessment model

Abstract

Network intrusion attempts have been on the rise recently. Researchers have shown an increased interest in assessing the security situation for entire network instead of single asset. A considerable amount of assessment models have been designed. However, there is a lack of solid and standard guidelines to define the importance of network asset. In addition, based on our knowledge, no research has been found that adequately covered the cost factor in the assessment model. Thus, the purpose of this paper is to propose a cost-sensitive entropy-based network security situation assessment model. With the aid of Analytic Hierarchy Process (AHP), the model can quantitatively determine the importance of assets in the network by considering the tangible and intangible criteria. To verify the performance of proposed model, a simulation of National Advanced IPv6 Centre (NAv6)'s network environment has been setup. The simulation results regarding security situation in particular time-interval are promising. Hence, the proposed model is able to provide network administrator a more reliable reference before any further decision making for the organization's network.