Multiple software products often exist on the same server and therefore vulnerability in one product might compromise the entire system. It is imperative to perform a security risk assessment during the selection of the candidate software products that become part of a larger system. Having a quantitative security risk assessment model provides an objective criterion for such assessment and comparison between candidate software systems. In this paper, we present a software product evaluation method using such a quantitative security risk assessment model. This method utilizes prior research in quantitative security risk assessment, which is based on empirical data from the National Vulnerability Database (NVD), and compares the security risk levels of the products evaluated. We introduced topic modeling to build a security risk assessment model. The risk model is created using Latent Dirichlet Allocation (LDA) to classify the vulnerabilities into topics, which are then used as the measurement instruments to evaluate the candidate software product. Such a procedure could
supplement the existing selection process, to assist the decision makers to evaluate open-source software (OSS) systems, to ensure that it is safe and secure enough to be put into their environment. Finally, the procedure is demonstrated using an experimental case study.

References


Keywords