Abstract

Due to the widespread use of Internet services and applications, the number and sophistication of cyberattacks has increased. Attack path analysis is one of the common methodologies for protecting network infrastructure. As a robust tool for this approach, attack graphs are widely used in the cybersecurity community to model threats and perform security risk assessment. To capture uncertainties and stochastic behavior, it is a natural choice to transform the attack graph models to Bayesian networks for static and dynamic analysis through inference. Given the vulnerabilities and their correlations, Bayesian inference on attack graphs makes the estimation of the risk of compromising the components of the system possible and detects multi-step attacks spreading through the system. Numerous efforts have concentrated on formalizing attack graphs into a Bayesian attack graph and developing mechanisms for analysis. However the study about the assessment of the Bayesian attack graph's performance is still a potential work. This thesis focuses on assessing the inference performance of imperfect Bayesian attack graph by applying cross-entropy and Confusion Matrix. We conducted comprehensive experimental evaluations on two different Bayesian attack graphs to support the validity of the proposed metric assessment scores. Particularly, we assess the performance of the models under the impact of deviation between the true attack scenario and the Bayesian attack graph constructed by system administrators.