Résumé

Dans cette thèse, nous nous somme intéressés à la modélisation du problème de la corrélation d'alertes à base de modèles graphiques probabilistes. Nous avons constaté que les approches existantes de corrélation d'alertes, soit se basent sur des connaissances explicites d'experts, soit utilisent des mesures de similarité simples qui ne permettent pas de détecter des scénarios d'attaque. Pour cela, nous avons d'abord proposé une nouvelle modélisation de la corrélation d'alertes, basée sur les classifieurs Bayésiens naïfs, qui permet d'apprendre les coordinations entre les attaques élémentaires qui contribuent à la réalisation d'un scénario d'attaque. Notre modélisation nécessite seulement une légère contribution des connaissances d'experts. Elle tire profit des données disponibles et fournit des algorithmes efficaces pour la détection et la prédiction des scénarios d'attaque. Ensuite, nous avons montré comment notre approche de corrélation d'alertes peut être améliorée en prenant en considération les informations contextuelles codées en logiques de description, notamment dans le contexte d'une détection coopérative d'intrusions. Enfin, nous avons proposé plusieurs mesures d'évaluation pour un multi-classifieurs Bayésiens naïfs. Ceci est très important pour l'évaluation de notre approche de corrélation d'alertes car elle utilise un ensemble de classifieurs Bayésiens naïfs pour surveiller plusieurs objectifs d'intrusion en même temps.

Abstract

In this thesis, we focused on modeling the problem of alert correlation based on probabilistic graphical models. Existing approaches either require a large amount of expert knowledge or use simple similarity measures which are not enough to detect coordinated attacks. We first proposed a new modeling for the alert correlation problem, based on naive Bayesian classifiers, which can learn the coordination between elementary attacks that contribute to the achievement of an attack scenario. Our model requires only a slight contribution of expert knowledge. It takes advantage of available data and provides efficient algorithms for detecting and predicting attacks scenarios. Then we show how our alert correlation approach can be improved by taking into account contextual information encoded in description logics, particularly in the context of a cooperative intrusion detection. Finally, we proposed several evaluation measures for a naive Bayesian muti-classifiers. This is very important for evaluating our alert correlation approach because it uses a set of naive Bayesian classifiers to monitor multiple intrusion objectives simultaneously.