Proposition d'une nouvelle approche de détection d'intrusions basée sur les règles associatives génériques de classification

Imen Brahmi, Sadok Ben Yahia, Yahya Slimani

Département des Sciences de l'Informatique
Faculté des Sciences de Tunis
Campus Universitaire 1060 Tunis, Tunisie
{sadok.benyahia, yahya.slimani}@fst.rnu.tn

Résumé. Les systèmes de détection d'intrusions (SDIs) ont pour objectif la sécurité des réseaux informatiques. Dans ce papier, nous proposons une nouvelle approche de détection d'intrusions basée sur des règles associatives génériques de classification pour améliorer la qualité de la détection d'intrusions.

1 Introduction

Dans ce papier, nous proposons un nouveau système de détection d'intrusions, visant la diminution de génération de fausses alarmes et l'augmentation de détection de vraies intrusions. Nous montrons que l'utilisation des règles associatives génériques, de taille très compacte, permet d'atteindre ce double objectif. Les expérimentations que nous avons menées, montrent que l'approche proposée permet d'obtenir un SDI robuste avec un taux très élevé de détection de vraies intrusions.

2 Le système de détection d'intrusions IDS-GARC

Peu de travaux ont fait appel au concept des règles associatives dans le cadre de détection d'intrusions. Pour améliorer la qualité de détection d'intrusions, nous proposons un nouveau SDI appelé IDS-GARC (Intrusion Detection System based on Generic Association Rule with Classifier), dont l'objectif est de minimiser la génération de fausses alarmes et surtout l'augmentation de détection de vraies intrusions.

Le nouveau système IDS-GARC, dont l'architecture du IDS-GARC est décrite par la figure 1, dérive de l'application d'un processus, qui peut être résumé dans les quatre étapes suivantes :

- Pré-traitement des données : Nous discrétisons automatiquement des données de détection d'intrusions identifiées par des experts en sécurité informatique
- Génération de la base générique des règles associatives : En particulier, nous utilisons les règles génériques extraites de la base IGB (Gasmi et al., 2006)
- Sélection des règles associatives génériques de détection : Pour se faire, nous avons recours à la classification associative.
- Construction d'un classifieur : Pour détecter les nouvelles attaques, nous utilisons un classifieur appelé GARIDC (Generic Association Rule for Intrusion Detection based Classifier).

3 Evaluation expérimentale

Afin d'évaluer les performances du IDS-GARC, nous avons mené une série d'expérimentations sur une base de données orientée détection d'intrusions DARPA 98. Le choix de cette base s'explique par le fait puisqu'elle est fréquemment utilisée pour évaluer les performances des SDIs. Le tableau 1 présente les résultats obtenus en termes de taux de détection et de