Diagnostic multi-sources adaptatif
Application à la détection d'intrusion dans des serveurs Web

Thomas Guyet*, Wei Wang*,**
René Quiniou*, Marie-Odile Cordier*

*INRIA/IRISA - Université Rennes 1
{thomas.guyet, rene.quiniou, marie-odile.cordier}@irisa.fr,
http://www.irisa.fr/dream/Pages_Pros/Thomas.Guyet/
**Sophia Antipolis/INRIA
wwangemail@gmail.fr

Résumé. Le but d'un système adaptatif de diagnostic est de surveiller et diagnostiquer un système tout en s'adaptant à son évolution. Ceci passe par l'adaptation des diagnostiqueurs qui précisent ou enrichissent leur propre modèle pour suivre au mieux le système au fil du temps. Pour détecter les besoins d'adaptation, nous proposons un cadre de diagnostic multi-sources s'inspirant de la fusion d'information. Des connaissances fournies par le concepteur sur des relations attendues entre les diagnostiqueurs mono-source forment un méta-modèle du diagnostic. La compatibilité des résultats du diagnostic avec le méta-modèle est vérifiée en ligne. Lorsqu'une de ces relations n'est pas vérifiée, les diagnostiqueurs concernés sont modifiés.

Nous appliquons cette approche à la conception d'un système adaptatif de détection d'intrusion à partir d'un flux de connexions à un serveur Web. Les évaluations du système mettent en évidence sa capacité à améliorer la détection des intrusions connues et à découvrir de nouveaux types d'attaque.

1 Introduction

Les systèmes automatiques de surveillance sont de plus en plus répandus. Ils ont pour tâche d'émettre des alarmes lors de dysfonctionnements de systèmes aussi variés que les patients en unités de soins intensifs, les systèmes physiques (*e.g.* voitures, machines industrielles) ou informatiques (*e.g.* les serveurs Web). Si les données disponibles sur le fonctionnement des systèmes surveillés sont de plus en plus riches, et si les techniques de monitoring sont de plus en plus performantes, l'adaptation en ligne du monitoring reste un défi important pour assurer une surveillance précise, robuste, en continu et ne nécessitant que peu d'intervention humaine. En particulier, l'adaptation en ligne de ces systèmes doit permettre de :

– faciliter l'installation d'un système de surveillance en le laissant automatiquement s'adapter aux conditions particulières de son utilisation (*e.g.* adaptation aux caractéristiques physiologiques d'un patient),