Détection d'intrusions dans un environnement collaboratif sécurisé

Nischal Verma*, François Trousset**
Pascal Poncelet***, Florent Masseglia****

*IIT - Guwahati, Assam, India - nischaliit@gmail.com,
**LGI2P- Ecole des Mines d'Alès, Parc Scientifique G. Besse, 30035 Nîmes, France - trousset@ema.fr
***LIRMM UMR CNRS 5506, 161 Rue Ada, 34392 Montpellier Cedex 5, France - poncelet@lirmm.fr
****INRIA Sophia Antipolis, route des Lucioles - BP 93, 06902 Sophia Antipolis, France
florent.masseglia@sophia.inria.fr

Résumé. Pour pallier le problème des attaques sur les réseaux de nouvelles approches de détection d'anomalies ou d'abus ont été proposées ces dernières années et utilisent des signatures d'attaques pour comparer une nouvelle requête et ainsi déterminer s'il s'agit d'une attaque ou pas. Cependant ces systèmes sont mis à défaut quand la requête n'existe pas dans la base de signature. Généralement, ce problème est résolu via une expertise humaine afin de mettre à jour la base de signatures. Toutefois, il arrive fréquemment qu'une attaque ait déjà été détectée dans une autre organisation et il serait utile de pouvoir bénéficier de cette connaissance pour enrichir la base de signatures mais cette information est difficile à obtenir car les organisations ne souhaitent pas forcément indiquer les attaques qui ont eu lieu sur le site. Dans cet article nous proposons une nouvelle approche de détection d'intrusion dans un environnement collaboratif sécurisé. Notre approche permet de considérer toute signature décrite sous la forme d'expressions régulières et de garantir qu'aucune information n'est divulguée sur le contenu des différents sites.

1 Introduction

Le déploiement des ordinateurs et des réseaux a considérablement augmenté les risques causés par les attaques sur les systèmes informatiques qui deviennent un réel problème pour les entreprises et les organisations. Alors qu'auparavant de nombreuses attaques se focalisaient sur les serveurs Web car ils étaient souvent mal configurés ou mal maintenus, les attaques les plus récentes profitent des failles de sécurité des services ou applications Web qui sont plus vulnérables Heady et al. (1990); Graham (2001); Escamilla (1998). Pour pallier ce problème, de nouvelles approches appelées Systèmes de Détection d'Intrusions (SDI) ont fait leur apparition. Installés sur les réseaux, ils ont pour objectif d'analyser le trafic de requêtes et de détecter des comportements malveillants (e.g. Prelude-IDS, Snort). Ils peuvent être classés en deux grandes catégories (*e.g.* McHugh et al. (2000); Proctor (2001)) : les *systèmes de détection d'anomalies* qui cherchent à détecter les attaques et les *systèmes de détection d'abus* qui,