Analyse visuelle pour la détection des intrusions

David Pierrot, Nouria Harbi

Université Lumière Lyon 2, Laboratoire ERIC 69676 BRON Cedex, FRANCE
{david.pierrot1,nouria.harbi}@univ-lyon2.fr

Résumé. La démocratisation d'Internet, couplée à l'effet de la mondialisation, a pour résultat d'interconnecter les personnes, les états et les entreprises. Le côté déplaisant de cette interconnexion mondiale des systèmes d'information réside dans un phénomène appelé "Cybercriminalité". Nous proposons une méthode de visualisation de grands "graphes" et l'exploitation d'analyses statiques des flux permettant de détecter les comportements anormaux et dangereux afin d'appréhender les risques d'une façon compréhensible par tous les acteurs.

1 Introduction

De nos jours, le maintien opérationnel d'un Système d'Information est devenu un des critères essentiels pour toute entreprise, ou personne cherchant à délivrer un service, ou simplement souhaitant communiquer. Le côté déplaisant de l'interconnexion mondiale des Systèmes d'Information réside dans un phénomène appelé "Cybercriminalité". Des personnes, des groupes mal intentionnés ont pour objectif de nuire aux informations d'une entreprise, d'une personne voire d'un Etat. Conséquemment, la détection des intrusions doit permettre de protéger le Système d'Information. L'objectif de cet article est de présenter dans un premier temps l'état de l'art en matière de détection d'intrusions et dans un second temps d'aborder les travaux menés afin de faciliter la visualisation des flux. La première partie de cet article sera consacrée à l'étude de l'existant dans laquelle nous présenterons les différentes approches de détection d'intrusions et leurs limites. Ensuite, nous nous intéresserons à la motivation de nos travaux et nous proposerons une solution. Nous détaillerons par la suite, la première phase de nos travaux ainsi que les résultats et nous terminerons par une conclusion et les perspectives.

2 Étude de l'existant

Une multitude d'outils (Antivirus, IDS, IPS, HIDS, Firewall) permettent aujourd'hui de mettre en place une sécurité "relative" pour l'ensemble du Système d'Information. Les principaux risques résiduels sont l'absence de constat en temps réel sur le signalement des comportements anormaux et sur l'exploitation des vulnérabilités. Il convient donc de répondre en fournissant des contremesures dans des délais raisonnables.

2.1 Les différentes solutions de détection d'intrusions

Les systèmes de détection des intrusions sont divisés selon les 3 familles distinctes :