Détection dans du trafic chiffré

Pierre-Olivier Brissaud
Doctorant
Thales Service (Theresis et Inria Nancy (Madynes)
Email : pierre-olivier.brissaud@inria.fr

***Abstract*—L'utilisation du chiffrement est en augmentation continue de nos jours et cela à des répercussions sur les mesures de sécurité qui existait jusqu'alors. Nous développerons ici les techniques existantes pour assurer la sécurité des systèmes malgré le chiffrement. La solution du proxy de coupure, bien que simple, n'est pas forcement une alternative satisfaisante à cause des problèmes de confidentialité qu'elle engendre. Des solutions alternatives existent sous forme de middlebox qui utilisent du chiffrement recherchable pour jouer un rôle équivalent au proxy mais qui assurent plus de confidentialité.**

L'autre alternative pour avoir un moyen non intrusif, est l'utilisation de l'analyse de trafic. Cela permet via l'unique observation des flux réseau de récupérer de l'information sur ce dernier sans opérer de déchiffrement. C'est souvent suffisant pour certaines taches telle que le black-listing de site web, exemple que nous approfondirons par la suite.

Keywords*—*Trafic Chiffré, Analyse de Trafic, Détection