Proposition de recherche doctorale

Description des attaques: Classification, formalisme et architecture de détection

Mots clés :

- **Directeur de thèse** : AHMED SERHROUCHNI
- **Co-encadrant(s)** :
- **Unité de recherche** : Laboratoire Traitement et Communication de l'Information
- **Ecole doctorale** : École Doctorale Informatique, Télécommunications, Électronique de Paris
- **Domaine scientifique principal**: Divers

Résumé du projet de recherche (Langue 1)

Les attaques sur les systèmes d'information en général et sur les applications web en particulier ont augmenté considérablement et sont devenues de plus en plus complexes et hétérogènes. Pour répondre à des besoins particuliers de sécurité, différentes plateformes de sécurisation ont été conçues : Firewall, IDS (Intrusion Detection System), WAF (Web Application Firewall), etc. Chaque plateforme dispose de son propre formalisme pour l'analyse et le filtrage des données protocolaires. Ces formalismes sont en général opaques et dépendent de l'éditeur de la plateforme quant à l'expression des règles de sécurité. En plus, ils sont souvent complexes et spécifiques à certains types d'attaques. C'est dans ce contexte que s'effectue notre thèse qui a pour objectif la définition, la conception et l'implémentation d'un langage dédié. Ce langage offrira un niveau d'abstraction assez élevé pour s'affranchir des contraintes liées à l'architecture et l'environnement d'exécution. L'apport de la thèse réside en la conception d'une solution permettant une écriture plus simple des règles de sécurité afin de proposer un format de règle mieux adapté aux besoins industriels.