Thèse : Détection d'attaques dans les réseaux de nouvelle génération grâce à l'IA symbolique

Directeur de thèse : Philippe Owezarski – LAAS-CNRS (owe@laas.fr)

Sujet :

Les réseaux de nouvelle génération, notamment cellulaires (5G, 6G), sont conçus pour être des réseaux multi-services proposant différentes classes de services, des services de slicing, … et surtout, vu leur importance stratégique, être sécurisés. Architecturalement, ces réseaux ne sont plus monolithiques en adoptant massivement le concept de fonctions réseaux virtualisées (NFV : Network Function Virtualization). Ils adoptent ainsi une architecture orientée microservices inspirée du cloud, ces microservices étant généralement supportés par des containers. Avec une telle architecture logicielle des nouveaux réseaux, leur surface d'attaque s'en trouve fondamentalement étendue, ouvrant la possibilité à de toutes nouvelles attaques ciblées, en plus des attaques traditionnelles qui existaient déjà pour les réseaux à architectures monolithiques.

Face à ces menaces, la détection d'attaques fait aujourd'hui appel à des techniques d'intelligence artificielle (IA), principalement des techniques d'apprentissage automatique reposant donc sur des modèles statistiques de métriques du trafic. Les bénéfices sont certains. Toutefois, ces techniques à base d'apprentissage automatique détectent des anomalies dans le trafic sans être capables de les classifier : anomalies bénignes, ou au contraire malicieuses, types d'attaques, etc. Ces nouvelles techniques, sont la plupart du temps incapables d'identifier l'intention derrière une séquences de paquets, flux ou événements.

Pour corriger ces limites, cette thèse propose d'ajouter aux techniques d'apprentissage automatique, des techniques d'IA symboliques pour permettre la reconnaissance de ces séquences et leur classification pour des contre-mesures correctement adaptées.