

Thèse : Cybersécurité, datasets et IA générative

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

Sujet :

La cybersécurité repose aujourd’hui de plus en plus sur des outils utilisant des techniques d’intelligence artificielle (IA), notamment d’apprentissage automatique. Pour fonctionner, ces techniques ont besoin d’un entraînement sur des données labélisées, les labels indiquant la nature des paquets et des flux du dataset : bénin et son type ou attaque et son type. Pour un bon entraînement des outils d’apprentissage automatique, les datasets doivent donc contenir une grande variété de trafics différents avec des attributs les caractérisant couvrant un large spectre de situations. L’objectif est de disposer de datasets permettant une évaluation complète et pertinente des outils de cybersécurité en évitant des erreurs liées à des phénomènes comme le sous- ou sur-apprentissage, par exemple.

Cette thèse a pour objectif d’étudier les possibilités de l’IA générative pour :

1. Générer des datasets de qualité permettant d’évaluer de façon pertinente et complète des outils de cybersécurité.
2. Concevoir de nouveaux outils de détection d’attaques qui seraient robustes à des attaques générées par des outils d’IA ou par des techniques d’apprentissage adverse (« adversarial learning »).

Cette thèse fera la part belle à des travaux de recherche expérimentale. Ainsi, l’identification des paramètres caractéristiques d’un dataset adapté à l’évaluation d’outil de cybersécurité à base d’IA se fera à partir de l’étude des datasets publics actuels et des résultats obtenus par des outils de détection d’attaques sur ces datasets. A partir de ces résultats, il faudra identifier les attributs caractéristiques permettant de distinguer le trafic bénin du trafic des attaques, et des attaques entre elles. Il faudra également définir les métriques permettant de caractériser et quantifier des éléments comme la variété, la variabilité, le niveau de couverture, etc. Il faudra également identifier comment une attaque pourra utiliser l’intelligence artificielle pour duper les systèmes de cybersécurité, et proposer des contre-mesures.