Collaboration fiable et confidentielle pour la détection dans les systèmes répartis

Léo Lavaur*[1]

[1]Interdisciplinary Centre for Security, Reliability and Trust (SnT) [University of Luxembourg] (SnT [uni.lu]) – Université du Luxembourg [Siège] – 2, place de l'Université – L-4365 Esch-sur-Alzette – Luxembourg, Luxembourg

Résumé

L'apprentissage fédéré a relancé l'intérêt pour les systèmes de détection d'intrusions collaboratifs, limités jusqu'alors par le risque de divulgation de données associé au partage d'informations. Est-ce pour autant un bon outil collaboratif ? Pensé à l'origine pour entrainer des modèles de prédiction sur les données de clients sans compromettre leur confidentialité, son usage comme outil de partage de connaissance entre des acteurs identifiés a été moins étudié. Dans cette présentation, je présenterai nos travaux sur l'apprentissage fédéré comme outil de collaboration entre acteurs institutionnels et les verrous associés, particulièrement sur la confiance entre acteurs dans un contexte hétérogène. Je présenterai ensuite nos travaux actuels sur l'usage de l'intelligence artificielle neurosymbolique et les possibilités que cela offre pour la sécurité. Enfin, nous regarderons les pistes ouvertes par ces travaux, et particulièrement ce qui nous sépare d'un système collaboratif fiable et interprétable qui respecte des contraintes fortes de confidentialité.

*Intervenant