N° d'ordre : D -

THESE

présentée

devant l'Institut National des Sciences Appliquées de Rennes

en vue de l'obtention du

DOCTORAT

spécialité : Image, Signal et Vision

par M SOURBIER Nicolas

Intitulé : **Détection d'intrusion réseau par apprentissage machine, un problème temps réel, déséquilibré et en constante évolution**

Directeur de Thèse : Maxime PELCAT

Date, heure et lieu de soutenance : 29/09/2022, 14h, Amphi Bonnin, Campus de l'INSA de RENNES,
20 Av. des buttes de Coësmes, 35708 Rennes.

Membres du jury :

Rapporteur: Isabelle Chrisment, Professeur des Universités, Université de Lorraine, LORIA.
Rapporteur: Malcolm Heywood, Professeur, Dalhousie University.
Examinatrice: Peggy Cellier, Maîtresse de Conférences HDR, INSA Rennes, IRISA.
Examinateur: Gilles Grimaud, Professeur des Universités, Université de Lille, CRIStAL.
Examinateur: Grégory Blanc, Maître de Conférences, SAMOVAR, IMT/Télécom SudParis, Institut Polytechnique de Paris.
Directeur: Maxime Pelcat, Maître de Conférence HDR, INSA Rennes, IETR.

RESUME DE LA THESE

Les systèmes de détection d'intrusion réseau (NIDS) observent le trafic réseau et essayent d'en extraire les intrusions : des compromissions de l'intégrité, la disponibilité ou la confidentialité des services et des données fournies par ce réseau.
Il existe deux types de NIDS. 1) Les systèmes de détection d'intrusion par signature identifient les intrusions connues en se référant à une base de connaissance existante. 2) Les systèmes de détection d'intrusion par anomalie qui qualifient les intrusions en se basant sur un modèle du trafic réseau normal, généralement appris par des techniques d'apprentissage machine.

La détection d'intrusion dans les réseaux comporte des verrous pour être déployée en pratique. Premièrement, la collecte de données réseau représentatives, réalistes et correctement étiquetées est complexe et coûteuse. Ces données sont également fortement déséquilibrées, les attaques étant des événements rares. Enfin, le portage opérationnel d'un AIDS appris peut entraîner une chute des taux de détection à cause de différences entre le contexte d'apprentissage et le contexte d'inférence.

Ce manuscrit explore les apports des Tangled Program Graphs (TPGs) au domaine de la détection d'intrusion par anomalies et montre que les TPG sont prometteurs pour la levée des verrous du domaine.