Détection d'anomalies explicable et transférable pour la cybersécurité dans un écosystème immunitaire artificiel

Explainable and transferable Anomaly Detection for cybersecurity in an Artificial Immune Ecosystem

ANR Artic Project, program « contrats doctoraux en intelligence artificielle »

Lieu de travail Strasbourg - Grand Est - France
Champs scientifiques Informatique
Direction : Pierre Parrend, Prof. HDR, ECAM Strasbourg-Europe
Co-Direction : Aline Deruyver, McF HDR, Université de Strasbourg

Mots clés

IA explicable; IA transférable; Détection d'anomalies; cyber-attaques complexes

Description

L'écosystème immunitaire artificiel prend en charge la détection, la mémoire et la tolérance pour détecter les attaques de cybersécurité complexes comme les attaques à étapes multiples ou à jour zéro. La détection identifie des modèles inhabituels susceptibles d'être un comportement malveillant. La mémoire stocke ces modèles pour une dernière détection. La tolérance utilise les commentaires d'experts et le stockage des modèles non malveillants antérieurs pour réduire les faux positifs.
Pour soutenir un processus d'analyse et de réaction efficace, les modèles extraits pour un écosystème informatique donné doivent présenter deux propriétés clés en intelligence artificielle: l'explicabilité et la transférabilité. L'explicabilité garantit que l'administrateur de cybersécurité dispose de suffisamment d'informations pour identifier, caractériser et réagir au trafic suspect. La transférabilité tire parti des
connaissances recueillies dans un contexte donné pour amorcer l'analyse dans un autre. Cela nécessite 1) que le modèle puisse être extrait et 2) qu'il puisse être adapté à un nouvel environnement, en éliminant les détecteurs spécifiques au système et en soutenant l'adaptabilité pour identifier de nouvelles anomalies.
À la suite d'une revue de la littérature sur l'intelligence artificielle explicable et transférable pour la cybersécurité, un nouveau modèle sera proposé et évalué par rapport à des algorithmes de pointe. Les réseaux de neurones (par ex: MLP) et les approches à arbres (par: Isolation forrests), qui présentent tous deux des avantages de performance majeurs pour la détection tout en ayant des conditions préalables
très distinctes sur la disponibilité des données et la puissance de calcul requise, seront considérés en priorité. Le cas échéant, ce modèle sera proposé pour de sconcours de cybersécurité ou de datascience.

Références

Fabio Guigou, 'The artificial immune ecosystem : a scalable immune-inspired active classifier, an application to streaming time series analysis for network monitoring', Université de Strasbourg, Thèse de doctorat, 18 juin 2019
P. Parrend, J. Navarro, F. Guigou, A. Deruyver, P. Collet, Foundations and Applications of Artificial Intelligence for Zero-day and Multi-Step Attack Detection, EURASIP Journal on Information Security, Springer, page 29, 2018
F. Guigou, P. Collet, P. Parrend, SCHEDA: lightweight euclidean-like heuristics for anomaly detection in periodic time series, Applied Soft Computing, Elsevier, Volume 82, septembre 2019

Compétences

Les compétences suivantes sont un critère de sélection important pour ce projet de thèse:

- Machine learning
- Ou: Statistiques pour la data sciences

Des connaissances théoriques ainsi qu'une première expérience pratique sont attendues.
Des compétences en théorie des graphes, ou en cybersécurité, sont un atout pour ce projet.
Les compétences rédactionnelles en anglais (et pour les candidats dont c'est la langue maternelle en français) sont très importantes pour la réussite d'une thèse de doctorat en informatique.

Expertises

Les expertises scientifiques qui seront acquises sont les suivantes:

- Explicabilité et transférabilité de l'intelligence artificielle
- détection d'anomalies
- caractérisation des attaques informatiques complexes

Le doctorat permet également de développer des compétences suivantes:

- autonomie et capacité d'initiative
- capacité d'analyse et de résolution de problèmes complexes
- expérience rédactionnelle en anglais (et français)
- aisance dans la communication de sujet techniques ou scientifiques

Candidature

Merci de nous faire parvenir un CV ainsi que les relevés de notes de Master/école d'ingénieur, ainsi que les classements, par mail : pierre.parrend@unistra.fr.
D'éventuelles publications scientifiques (y compris rapports scientifiques non publiés) sont un plus dans la candidature.

Description

The Artificial Immune Ecosystem supports detection, memory and tolerance for detecting complex cybersecurity attacks like multi-step or zero-day attacks.
Detection finds unusual patterns likely to be a malicious behaviour. Memory stores these patterns for latter detection. Tolerance uses expert feedback and storage of earlier non-malicious patterns to reduce false positives.
To support an efficient analysis and reaction process, the models extracted for a given IT ecosystem must exhibit two key properties of artificial intelligence: explainability and transferability. Explainability ensures that the cybersecurity administrator have enough information to identify, characterize and react to suspicious traffic. Transferability leverages the knowledge gathered in one given context to bootstrap analysis in another. It requires 1)that the model can be extracted and 2)that it can be tailored to a new environment, abstracting away system-specific detectors and supporting adaptability to identify new anomalies.
Following a literature review on explainable and transferable Artificial Intelligence for Cybersecurity, a new model will be proposed and evaluated wrt. state of the art algorithms. Neural networks (such as MLP) and tree-based approaches (such as Isolation Forrests), which both exhibit major performance benefits for detection while having very distinct pre-conditions on data availability and required computing power, will be considered in priority. If relevant, this model will be challenged through cybersecurity or datascience competitions.

Keywords

Explainable AI; Transferable AI; Anomaly detection; complex cyber attacks

References

Fabio Guigou, 'The artificial immune ecosystem : a scalable immune-inspired active classifier, an application to streaming time series analysis for network monitoring', Université de Strasbourg, Thèse de doctorat, 18 juin 2019

P. Parrend, J. Navarro, F. Guigou, A. Deruyver, P. Collet, Foundations and Applications of Artificial Intelligence for Zero-day and Multi-Step Attack Detection, EURASIP Journal on Information Security, Springer, page 29, 2018

F. Guigou, P. Collet, P. Parrend, SCHEDA: lightweight euclidean-like heuristics for anomaly detection in periodic time series, Applied Soft Computing, Elsevier, Volume 82, septembre 2019

Skills

The following skills are an important selection criterion for this thesis project:

- Machine learning
- Or: Statistics for data science

Theoretical knowledge as well as a first practical experience are expected.
Skills in graph theory, or cybersecurity, are an important asset.
Writing skills in English (and for native speakers in French) are very important for the success of a doctoral thesis in computer science.

Expertises

The scientific expertise that will be acquired is as follows:

- Explicability and transferability of artificial intelligence
- anomaly detection
- characterization of complex computer attacks

The doctorate also helps develop the following skills:

- autonomy and capacity for initiative
- ability to analyze and solve complex problems
- writing experience in English (and French)
- proficiency in communicating technical or scientific subjects

Applications

Please send us a CV as well as the Master / engineering school transcripts, as well as your rankings, by email to: pierre.parrend@unistra.fr.

Any scientific publications (including unpublished scientific reports) are a plus in the application.