DynAISEC

Adaptive AI/ML for Dynamic Cybersecurity Systems

Programm / Ausschreibung	IKT der Zukunft, IKT der Zukunft, IKT der Zukunft - 9. Ausschreibung (2020)	**Status**	abgeschlossen
Projektstart	14.01.2022	**Projektende**	13.07.2024
Zeitraum	2022 - 2024	**Projektlaufzeit**	31 Monate
Keywords	security, AI/ML, threat detection, anomaly detection, adaptive and incremental learning, synthetic data		

Projektbeschreibung

Cybersecurity ist unabdingbar für unserer digitale Gesellschaft. Der zunehmende Anteil an mobiler Kommunikation, die Vielzahl an heterogenen, miteinander verbundenen Geräten (IoT, Smartphones, M2M etc.), die wachsende Zahl an kritischen Infrastrukturen, die das Internet nutzen (z.B. e-Health, Finanzwesen, Verwaltung), sowie der gesellschaftliche Umbruch zu „all-remote im Zuge der Corona-Pandemie haben die Entwicklung neuer digitaler Bedrohungen und Angriffe gegen alle möglichen Systeme und Unternehmen weiter befeuert. Deren Bewältigung erfordert daher bessere, effizientere und robustere Ansätze in der Cybersecurity. Darüber hinaus hat der im letzten Jahrzehnt beachtliche Erfolg von Artificial Intelligence und Machine Learning für verschiedenste datengestützte Probleme eine florierende Forschungslandschaft rund um die Anwendung von AI/ML in der Cybersecurity – AISEC – hervorgebracht. Die Übertragung von AISEC in die Praxis ist jedoch nach wie vor äußerst anspruchsvoll.
Das DynAISEC-Projekt setzt sich zum Ziel, die AISEC entscheidend voranzutreiben. In erster Linie möchten wir den Mangel an Ansätzen für adaptives und inkrementelles Lernen beheben, der dafür sorgt, dass gegenwärtige AISEC-Ansätze nicht mit der Dynamik von Cyber-Angriffen und Netzwerkverkehr mithalten können. Die überwiegende Anzahl bisheriger AI4SEC-Modelle wird offline trainiert und bleibt im Fall von bisher unbekannten Angriffen (--> hohe False-Negative-Rate) oder in Szenarien mit dynamischer Baseline (--> hohe False-Positive-Rate) hinter den Erwartungen zurück. Um inkrementelles Lernen zu ermöglichen, müssen AI4SEC-Modelle erneut trainiert werden, sobald jüngere Daten zur Verfügung stehen. Wie das umgesetzt werden kann, ist eine offene Forschungsfrage. In diesem Projekt werden wir daher die GenDeX-Technologie erforschen und entwickeln. GenDex ist ein kombinierter Ansatz für adaptive Cybersecurity bestehend aus drei wesentlichen Bestandteilen: (i) der automatischen und kontinuierlichen Erzeugung von synthetischen Daten mit generativen Modellen als Eingabedaten für das datengestützte Lernen; (ii) dem kontinuierlichen Erkennen von Angriffen und Anomalien durch neue AI4SEC-Modelle, die jüngste Entwicklungen der AI/ML nutzen, sowie die Erkennung von sogenannten „Concept Drifts“ (d.h. Änderungen in der Statistik der zugrundeliegenden Daten), um den richtigen Punkt für das Re-Training zu erkennen; (iii) die automatische Erklärung von AI4SEC-Entscheidungen bei der Erkennung von sowohl Angriffen als auch Drifts, um das Verständnis von und Vertrauen in AI4SEC zu erhöhen sowie schnellere Diagnosen und Entscheidungen zu ermöglichen.
Die erwarteten Ergebnisse sind: (i) datengetriebene AI4SEC-Modelle mit adaptiven Fähigkeiten für verbesserte Cybersecurity-Performance (höhere Erkennungsraten bei reduzierten, falschen Alarmen); (ii) Algorithmen für die

automatische Generierung von synthetischen Cybersecurity-Daten für adaptives Re-Training mit Garantien bzgl. der Korrektheit der synthetischen Daten; (iii) Software-Bibliotheken, die die Erklärung von Modelverhalten und erlauben; (iv) Prototypen für drei spezifische Szenarien, nämlich In-Network Security (Verbreitung von Malware, IoT-targeted attacks, DDoS-Angriffe), Web-browsing End User Security (Phishing, Fake-Site-Erkennung, Privacy Leaks, Data Exposure von MitarbeiterInnen) sowie In-Device Security von mobilen Geräten (Malware Erkennung auf Smartphones).

Abstract

Cybersecurity is a cornerstone to our digital society. The rise of ubiquitous mobile communications, the plethora of heterogeneous interconnected devices (IoT, smartphones, M2M, etc.), the growing number of critical infrastructures served over networks (e-health, finances, governance, etc.), and the massive shift of society to an all-remote paradigm induced by the covid-19 pandemic have nothing but accelerated the pace of new cyber threats and the realization of cyber-attacks impacting all sorts of systems and enterprises, calling for better, more efficient, and more robust approaches to cybersecurity. The impressive success of Artificial Intelligence and Machine Learning in multiple data-driven problems over the past decade has motivated a flourishing research domain targeting the application of AI/ML to cybersecurity problems - AI4SEC. However, making of AI4SEC an accepted and fruitful approach to cyber security in the practice has proven extremely challenging.

The goal of DynAISEC is to significantly advance the AI4SEC domain, tackling one particularly complex deficiency faced by currently proposed solutions, which limits their application in the practice: the lack of adaptive and incremental learning to deal with the dynamic nature of cyber-attacks and networking data. Most AI4SEC models are trained offline, causing them to underperform in the event of previously unseen attacks (high rates of false negatives) or under dynamic baseline scenarios (high false alarm rates). The ability to retrain AI4SEC models as new data is generated is fundamental to achieve adaptive incremental learning, which remains an open research direction. To tackle this limitation, we propose to research and develop the GenDeX technology: GenDeX stands for a combined approach to adaptive cybersecurity, spanning three key components: (i) the automatic and continuous Generation of synthetic cybersecurity data through generative models - synthetize input data in controlled yet heterogeneous scenarios to enhance data-driven learning; (ii) the continuous Detection of attacks and anomalies through novel AI4SEC models – from Deep to Graph-based learning architectures – exploiting recent advancements in AI/ML, as well as the Detection of so-called concept-drifts - changes in the underlying statistics of the analyzed data (either attacks or baseline), to decide for the right times to (incrementally) re-train the conceived AI4SEC models; and (iii) the automatic eXplanation of both AI4SEC detection decisions as well as concept drift detections, to further increase understanding and trust on AI4SEC, additionally enabling faster means for diagnosis and decision making.

The expected results of DynAISEC are: (i) data-driven AI4SEC models with adaptive capabilities for enhanced cybersecurity performance (higher detection rates with lower false alarms); (ii) algorithms for the automatic synthetization of cybersecurity data for adaptive model re-training, offering data curation warranties – i.e., the correctness of the synthesized data; (iii) software libraries providing explainability of model behaviours and predictions; and (iv) multiple prototype demonstrators targeting three specific cybersecurity scenarios, including in-network security (malware propagation, IoT targeted attacks. DDoS attacks), web-browsing end user security (phishing attacks, fake site detection, privacy leakage, employee data exposure), and in-device security for mobile devices (malware detection in smartphones).

Projektkoordinator

- Universität Wien

Projektpartner

- SBA Research gemeinnützige GmbH
- AIT Austrian Institute of Technology GmbH
- cyan Security Group GmbH