UNIVERSITÄT
LIECHTENSTEIN

Medienmitteilung der Universität Liechtenstein
20. Juli 2022

Forscher der Universität Liechtenstein erhält den renommierten „Test of Time“-Award

Prof. Dr. Pavel Laskov, Inhaber des Hilti Lehrstuhls für Daten- und Anwendungssicherheit an der Universität Liechtenstein, wurde gemeinsam mit seinen Co-Autoren Prof. Battista Biggio, Universita di Cagliari, Italien, und Dr. Blaine Nelson, Robust Intelligence, USA, der renommierte Preis „Test of Time“ auf der International Conference on Machine Learning (ICML) am 19. Juli 2022 verliehen.

Der „Test of Time“-Preis wird seit 2010 auf der ICML verliehen und zeichnet jene Arbeiten aus, die in den zehn Jahren seit ihrer Präsentation an der ICML den grössten Einfluss auf die wissenschaftliche Gemeinschaft erzielt haben. In diesem Jahr ging der Award an Prof. Dr. Pavel Laskov und seine Co-Autoren für ihren Artikel „Poisoning Attacks against Support Vector Machines“, der als bedeutendster von insgesamt 244 Beiträgen, die auf der ICML 2012 präsentiert worden waren, eingestuft wurde. Die Autoren reihen sich damit unter Forscher der University of Amsterdam, ETH Zürich, Harvard University, Amazon Research, INRIA, Facebook Research, Google Brain und DeepMind, die den Preis in den vergangenen fünf Jahren erhielten.

Worum ging es in dem preisgekrönten Artikel?
Die Algorithmen des Maschinellen Lernens haben sich bereits zu Anfang der 2000er-Jahre als das wichtigste Instrument für Datenanalyse in diversen Internet-Technologien etabliert. So spielen sie auch eine wichtige Rolle in modernen Sicherheitstechniken, z.B., um neue Bedrohungen zu erkennen oder sich ständig verändernde Phishing-Seiten zu enttarnen. Bereits 2006 wurde allerdings angedeutet, dass die Angreifer die lernbasierten Erkennungstechniken durch die Manipulation von ihren Daten überwinden können – auch wenn die ersten solchen Angriffe gegen sehr einfachen Lernalgorithmen ausgerichtet wurden . „Können die Angriffe durch manipulierte Daten auch die Mainstream-Algorithmen überwinden, die deutlich komplexer sind?“, fragten sich 2011 Laskov, Biggio und Nelson, die damals gemeinsam an der Universität Tübingen in Deutschland arbeiteten. 2013 konzipierten die gleichen Autoren auch den ersten Angriff der ein bereits trainiertes Modell umgehen konnte. 2014 wurde der gleiche Phänomen in einer anderen Arbeit von Forschern aus Google, New York University und University of Montreal unabhängig aufgedeckt und als „verblüffende Eigenschaften“ von Neuronale Netzen interpretiert.
Seitdem erschienen mehr als 5000 Artikel in Fachzeitungen und Konferenzen, in denen die Sicherheit von Künstlicher Intelligenz untersucht wird. Auch laufende Arbeiten von Pavel Laskov und seinen Kollegen am Hilti-Lehrstuhl für Daten- und Anwendungssicherheit befassen sich unter anderem mit solchen Themen; deren jungster Artikel über die Sicherheit von KI-Komponenten in 5G-Netzinfrastrukturen im IEEE Journal on Network and Service Management erschien und in Nachrichten von TechTarget, einem einflussreichen IT-Marketing-Dienst, als potenzielle neue Bedrohung für 5G-Technologien hervorgehoben wurde.

Was bedeutet diese Forschungsarbeit für Liechtenstein?
Die in der Arbeit von Pavel Laskov ausgezeichneten Ergebnisse dienen primär der Grundlagenforschung. Sie zeigen auf, dass die Universität Liechtenstein über die Expertise verfügt, um in der Lehre und in weiteren Forschungsprojekten auf den Gebieten von Cybersicherheit und Data-Science auf weltweit

Kontakt: Heike Esser / Kommunikation & Marketing
Universität Liechtenstein / Fürst-Franz-Josef-Strasse / 9490 Vaduz, Liechtenstein
Telefon +423 265 11 11 / Direkt +423 265 13 31 /heike.esser@uni.li / www.uni.li

höchstem Niveau zu agieren. Der Praxisbezug für die Sicherheit Künstlicher Intelligent lässt zudem nicht lange auf sich warten. Im Vorschlag der Europäischen Kommission für den Rechtsrahmen für Künstliche Intelligenz wird die Resilienz gegen Poisoning- und Manipulationsangriffe als wesentliche Anforderung für die sogenannten „High-Risk-Anwendungen“ der Künstlichen Intelligenz erwähnt – Umsetzungsfrist ist voraussichtlich bereits 2024.

1457 Zeichen (inkl. Leerzeichen)

Kontakt: Heike Esser / Kommunikation & Marketing
Universität Liechtenstein / Fürst-Franz-Josef-Strasse / 9490 Vaduz, Liechtenstein
Telefon +423 265 11 11 / Direkt +423 265 13 31 / heike.esser@uni.li / www.uni.li