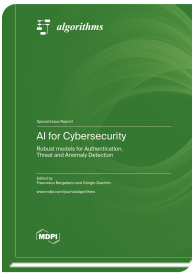
algorithms

IMPACT FACTOR 1.8

CITESCORE 4.1

Special Issue Reprint

AI for Cybersecurity: Robust models for Authentication, Threat and Anomaly Detection



www.mdpi.com/books/reprint/7647

Edited by
Francesco Bergadano
Giorgio Giacinto

ISBN 978-3-0365-8264-1 (Hardback)
ISBN 978-3-0365-8265-8 (PDF)

Cybersecurity models include provisions for legitimate user and agent authentication, as well as algorithms for detecting external threats, such as intruders and malicious software. In particular, we can define a continuum of cybersecurity measures ranging from user identification to risk-based and multilevel authentication, complex application and network monitoring, and anomaly detection. We refer to this as the “anomaly detection continuum”. Machine learning and other artificial intelligence technologies can provide powerful tools for addressing such issues, but the robustness of the obtained models is often ignored or underestimated. On the one hand, AI-based algorithms can be replicated by malicious opponents, and attacks can be devised so that they will not be detected (evasion attacks). On the other hand, data and system contexts can be modified by attackers to influence the countermeasures obtained from machine learning and render them ineffective (active data poisoning). This Special Issue presents ten papers that can be grouped under five main topics: (1) Cyber–Physical Systems (CPSs), (2) Intrusion Detection, (3) Malware Analysis, (4) Access Control, and (5) Threat intelligence.
AI is increasingly being used in cybersecurity, with three main directions of current research: (1) new areas of cybersecurity are being addressed, such as CPS security and threat intelligence; (2) more stable and consistent results are being presented, sometimes with surprising accuracy and effectiveness; and (3) the presence of an AI-aware adversary is recognized and analyzed, producing more robust solutions.

MDPI

MDPI Books

Publishing Open Access Books & Series

MDPI Books offers quality open access book publishing to promote the exchange of ideas and knowledge in a globalized world. MDPI Books encompasses all the benefits of open access – high availability and visibility, as well as wide and rapid dissemination. With MDPI Books, you can complement the digital version of your work with a high quality printed counterpart.

Open Access

Your scholarly work is accessible worldwide without any restrictions. All authors retain the copyright for their work distributed under the terms of the Creative Commons Attribution License.

Author Focus

Authors and editors profit from MDPI's over two decades of experience in open access publishing, our customized personal support throughout the entire publication process, and competitive processing charges as well as unique contributor discounts on book purchases.

High Quality & Rapid Publication

MDPI ensures a thorough review for all published items and provides a fast publication procedure. State-of-the-art research and time-sensitive topics are released with a minimum amount of delay.

High Visibility

Due to our global network and well-known channel partners, we ensure maximum visibility and broad dissemination. Title information of books is sent to international indexing databases and archives, such as the Directory of Open Access Books (DOAB), and the Verzeichnis Lieferbarer Bücher (VLB).

Print on Demand and Multiple Formats

MDPI Books are available for purchase and to read online at any time. Our print-on-demand service offers a sustainable, cost-effective and fast way to publish MDPI Books printed versions.

MDPI AG
Grosspeteranlage 5
4052 Basel
Switzerland
Tel: +41 61 683 77 34
www.mdpi.com/books
books@mdpi.com