DOI: doi.org/10.47363/JAICC/ICAIC2025/2025(4)16

International Conference on
Artificial Intelligence and Cybersecurity (ICAIC 2025)

Conference Proceedings

November 27-28, 2025 (Virtual)

Mitigating Cybersecurity Challenges from Software Misconfiguration with Bio-inspired Algorithm and Machine Learning

Shuvalaxmi Dass

School of Computing and Informatics, University of Louisiana at Lafayette, USA

Abstract

Software systems and applications are designed with many configuration parameters that contribute to various functionalities such as architecture, virtualization, performance, security, privacy, and system interactions. However, software misconfiguration can result in system vulnerabilities and susceptibility to security attacks. The Open Web Application Security Project, a nonprofit foundation, considers security misconfiguration as one of the top risks to cybersecurity. From a software testing perspective, it is infeasible to manually enumerate and verify all these configuration settings for vulnerability to attacks. Furthermore, software systems are generally built to operate with relatively static configurations over extended periods. This static approach can result in system vulnerabilities that may be exploited by adversaries during the reconnaissance stage, increasing the likelihood of successful attacks. In this talk, I will address the above cybersecurity challenges by applying bio-inspired algorithms and machine learning to enhance the security and robustness of software systems. First, I will introduce my novel concept of ?Vulnerability Coverage? as a software security testing strategy using bio-inspired algorithms. Next, I will present a ?Reinforcement Learning-based Game Model? to automate the dynamic Moving Target Defense (MTD) strategy for safeguarding vulnerable software from adversarial attacks. Finally, I will conclude my talk with exciting future directions in the field AI and evolutionary algorithms in cybersecurity.