Agentic AI and the Cyber Arms Race[*]

Keynote

Sean Oesch, Senior Scientist of Oak Ridge National Laboratories

In the early years of cybersecurity, defenders utilized virus-specific signatures, honeypots, and heuristics. As attacks increased in volume and attackers became more sophisticated, moving toward polymorphic malware, packers, and novel evasion techniques, defenders looked to machine learning to provide scalability (quickly analyze large volumes of data and automate repetitive tasks), pattern recognition (detect common attack patterns), and novelty detection (recognize abnormal behaviors that may indicate malicious actors or insider threats). With the advent of deep learning-based reinforcement learning algorithms and large language models we are on the cusp of another revolution in cybersecurity - agentic artificial intelligence. In this talk, Sean Oesch, a cyber researcher and senior scientist at Oak Ridge National Laboratory, will discuss the implications of agentic AI for cyber warfare and share his thoughts on how to educate AI savvy students who can defend the networks and critical infrastructure of the future.