VICEROY NORTHWEST INSTITUTE FOR CYBERSECURITY EDUCATION AND RESEARCH

CySER Virtual Seminar

Dr. Yong (Steve) Wang
Professor, University of Idaho

Securing Machine Learning: Evolving Threats, Attacks, and Defenses

Feb. 17, 2026, 1:10 – 2 PM Pacific

Team Link: Click here to join the meeting
Meeting ID: 212 501 175 374 68 | Passcode: wP2dk7MD
Call in (audio only) +1 509-498-6399 | Phone Conference ID: 136 940 281#

Abstract:

Machine learning (ML) has gained increasing attention in recent years, with applications spanning nearly every industry. However, its widespread adoption has also led to a rise in security threats. This presentation explores evolving threats, attacks, and defense strategies against adversarial attempts on ML models. Specifically, we will examine two types of adversarial attacks: exploration attacks targeting hypersphere-based ML models and exploitation attacks affecting both tree-based supervised and unsupervised ML models. Additionally, we will introduce defense mechanisms against adversarial attacks and discuss key challenges in securing machine learning systems.

Bio:

Dr. Yong Wang is a Professor and Chair in the Department of Computer Science at the University of Idaho. He holds a Ph.D. in Computer Science from the University of Nebraska–Lincoln and has over a decade of experience in the telecommunications industry prior to transitioning to academia. His research focuses on security and privacy in IoT, cyber-physical systems, cyberinfrastructure, and adversarial ML. He has published over 100 peer-reviewed papers and secured more than $2.5 million in research funding. Dr. Wang also serves as a commissioner for the ABET Computing Accreditation Commission. He is dedicated to student success, fostering collaboration, and driving innovation in computer science education and research.