Cybersecurity Analysis and Detection of Advanced Cyber Threats

John (Junghwan) Rhee, Ph. D.

Associate Professor, University of Central Oklahoma

jrhee2@uco.edu

Abstract

The frequency and sophistication of cybersecurity attacks targeting critical infrastructure, businesses, educational institutions, and government agencies continue to grow each year. Many of these attacks, such as ransomware and data breaches, are carefully orchestrated to remain stealthy and undetected over extended periods. These characteristics make detection and prevention particularly challenging, as malicious behavior is often obscured by legitimate system activity.

In this talk, Dr. Rhee will present a series of research projects focused on system-wide monitoring, behavioral analysis, and advanced threat detection. His work explores data-driven methods that trace causal chains of complex attack behaviors, as well as approaches that leverage domain knowledge of operating systems to identify anomalous states indicative of cyber threats. The talk will conclude with an overview of new cybersecurity programs being developed at the University of Central Oklahoma, which aim to provide students with practical, hands-on experience and foundational skills in cybersecurity.

Biography

Dr. Junghwan (John) Rhee is an Associate Professor in the Department of Computer Science at the University of Central Oklahoma. He earned his Ph.D. in Computer Science from Purdue University. Before joining UCO, he served for nine years as a senior researcher and security team leader at NEC Laboratories America in Princeton, New Jersey.

Dr. Rhee's research lies at the intersection of system security and reliability, with a focus on system diagnosis, end-host security, system provenance, and cyber-physical systems. His work is grounded in data-driven methodologies, program analysis, and operating systems techniques, aiming to enhance the detection and understanding of complex cyber threats. He has published 63 peer-reviewed conference papers, 5 journal articles, and holds 29 U.S. patents.

Two Decades of Applied AI: A Research Journey Through Security, Networks, and Language

Miguel Vargas Martin
Professor of Computer Science, Ontario Tech University

Abstract

This keynote traces a two-decade research journey at the intersection of machine learning, cybersecurity, human interaction, and natural language processing, shaped by the evolution of AI methods and their application to real-world challenges. While rooted in Dr. Vargas Martin's research, the talk reflects more broadly on how AI has matured as a powerful enabler of scientific inquiry and system design across domains. The journey began in 2006 with statistical learning techniques for detecting child sexual abuse material in network traffic, an early demonstration of AI in support of digital safety. In 2011, neural networks were applied to predict learner behaviour in digital environments, paving the way for future user modeling efforts. By 2015, the focus shifted to detecting covert side-channel communication in wireless and mobile ad hoc networks, where machine learning uncovered hidden signaling patterns within low-level protocols. From 2018 to 2022, the research moved increasingly toward human-centered security, investigating password memorability and later generating resilient authentication data using adversarial learning and pre-trained language models. In parallel, new directions emerged in affective computing, including the modeling of artificial empathy in clinical companion robots with privacy-by-design principles (2021), and the development of emotion recognition systems for social robots (2022). Most recently, the work has returned to foundational NLP problems, including enhanced sentence-wise text segmentation using transformer models (2024) and the application of large language models to detect cryptographic misuse in software systems (2025). Throughout this arc, machine learning has remained a constant, not merely as a method, but as a lens through which to interpret, model, and shape intelligent, secure, and human-aware systems. This talk will explore that continuum, situating past projects within the evolving landscape of AI and drawing lessons for future interdisciplinary research in the spirit of the SNPD community.

Biography

Miguel Vargas Martin is a Professor of Computer Science at Ontario Tech University. He holds a PhD in Computer Science from Carleton University, a Master's in Electrical Engineering from CINVESTAV-IPN, and a Bachelor's in Computer Science from UAA. A licensed Professional Engineer in Ontario, he has led over two decades of interdisciplinary research at the intersection of cybersecurity, machine learning, and human-computer interaction. His work has addressed challenges ranging from the detection of covert communication in wireless networks to password usability, AI-generated authentication artifacts, affective computing for social robots, and large language model applications in software security. Unifying these efforts is a long-standing focus on the responsible use of AI to build secure, intelligent, and human-aware systems.