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.