第2回研究領域セミナー

（次世代デジタル社会基盤研究領域）

テーマ

“Machine Learning and Cybersecurity: A Tale of Two Buzzwords”

講演者：Kansas 大学　教授　LUO, Bo　氏

日　　時：令和5年6月14日（水）16：00～17：00

場　　所：情報科学研究棟Ⅲ棟5階　コラボレーションルーム7

講演要旨：

Recent developments in machine learning have transformed many data analytic applications, such as speech recognition, computer vision, and natural language processing. ML also made its impact to the security and privacy community, for instance, in network intrusion detection, malware detection, and malicious behavior analysis. Meanwhile, a broad spectrum of cyber-attacks against machine learning systems has been proposed. Such attacks aim to break the integrity or confidentiality of the models. In this talk, I will introduce several research projects from KU’s InfoSec group: (1) AI/ML attack evaluation, (2) a highly effective and very stealthy neural Trojan, (3) an inversion attack against NLP model sharing, (4) a universal defense mechanism against adversarial ML attacks, (5) employing machine learning for mobile/IoT device recognition, and (6) using machine learning to examine privacy compliance for IoT apps. Through this talk, we hope to highlight the security and privacy issues in AI/ML systems, which may be helpful for the audience to identify the opportunities and challenges in their own research fields.

講演者略歴：

Bo Luo is a professor with the EECS department at the University of Kansas. He is the director of the Center for High Assurance and Secure Systems (HASS) at KU's Institute of Information Sciences (I2S). He received Ph.D. degree from The Pennsylvania State University in 2008, M.Phil degree from the Chinese University of Hong Kong in 2003, and B.E. from University of Sciences and Technology of China in 2001. His recent works mostly lie in the intersection of data science and privacy and security. Dr. Luo has published 90+ refereed papers, including ones in top conferences and journals such as IEEE S&P, ACM CCS, USENIX Security, ACM Multimedia, IEEE TKDE, IEEE TIFS, IEEE TDSC, VLDBJ, etc. He received the KU EECS Excellence in Undergraduate Teaching Professorship in 2023. He received the Miller Scholar award of University of Kansas in 2016, 2017, and 2021, and the Miller Professional Development Award in 2015. He is also the recipient of ACSAC 2017 and ACSAC 2021 best paper awards, and CCS 2022 best paper honorable mention.

会場での聴講を希望される方は下記お問合せ先までご連絡ください。

お問合せ先：共通事務管理課共通事務第二係（E-mail：is-secr@ml.jaist.ac.jp）