THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

Department of Computing
電子計算學系

Research Centre on Data Science & Artificial Intelligence
人工智能與數據科學研究中心
RC-DSAI

IEEE Computational Intelligence Society

Distinguished Seminar Series on Data Science & Artificial Intelligence

Challenges in AI Security

Prof. Dapeng Wu
Professor
Department of Electrical & Computer Engineering
University of Florida
USA

31 August 2021 (Tue)

10:00 – 11:00 (HKT, UTC+8)

Online via Zoom

English

Please register at https://polyu.hk/vUTxq or scan the QR code

All are welcome!

Abstract

With the recent breakthroughs, artificial intelligence, especially deep neural networks, is pervasively serving numerous areas such as healthcare, autonomous driving, and Internet of things. Deep neural networks are capable of making accurate predictions and reasonably good decisions but their predictions or decisions are not explicitly explainable. In particular, major security and privacy concerns exist in deep neural networks. In this talk, I will first provide an overview of trustworthy deep neural networks and then focus on our recent research on a data-agnostic model stealing attack. The talk will conclude by discussing future research directions in security and privacy concerns and potential countermeasures in deep neural networks.

About the Speaker

Dapeng Oliver Wu received Ph.D. in Electrical and Computer Engineering from Carnegie Mellon University, Pittsburgh, PA, in 2003. Since 2003, he has been on the faculty of Electrical and Computer Engineering Department at University of Florida, Gainesville, FL, where he is currently Professor. His research interests are in the areas of networking, communications, video coding, image processing, computer vision, signal processing, and machine learning. He received University of Florida Term Professorship Award in 2017, University of Florida Research Foundation Professorship Award in 2009, AFOSR Young Investigator Program (YIP) Award in 2009, ONR Young Investigator Program (YIP) Award in 2008, NSF CAREER award in 2007, the IEEE Circuits and Systems for Video Technology (CSVT) Transactions Best Paper Award for Year 2001, the Best Paper Award in GLOBECOM 2011, and the Best Paper Award in QShine 2006. He has served as Editor-in-Chief of IEEE Transactions on Network Science and Engineering. He was the founding Editor-in-Chief of Journal of Advances in Multimedia between 2006 and 2008, and an Associate Editor for IEEE Transactions on Communications, IEEE Transactions on Signal and Information Processing over Networks, IEEE Signal Processing Magazine, IEEE Transactions on Circuits and Systems for Video Technology, IEEE Transactions on Wireless Communications and IEEE Transactions on Vehicular Technology. He has served as Technical Program Committee (TPC) Chair for IEEE INFOCOM 2012. He was elected as a Distinguished Lecturer by IEEE Vehicular Technology Society in 2016. He is an IEEE Fellow.