香港浸會大學
HONG KONG BAPTIST UNIVERSITY

DEPARTMENT OF
COMPUTER SCIENCE
計算機科學系

ONLINE SEMINAR
2022 SERIES

Department of Computer Science

Dr. Chaowei Xiao

Assistant Professor
Arizona State University
United States

Register Now

Date: 17 February 2022 (Thursday)

Time: 11:00am – 12:00nn

Registration: http://bit.ly/bucs-ereg

(*Zoom details will only be provided to registrants)

Deep Learning in Adversarial Environments and Beyond

ABSTRACT

Deep Learning (DL) has achieved great success these days. It has been used in many applications in the real world, even in safety-critical applications such as autonomous driving systems. It seems that we are ready for DL now. However, is DL ready for us? In this talk, I will answer this question by exploring the threats of current DL systems in adversarial environments where adversaries could manipulate inputs. To raise awareness of this threat and motivate the investigation of defense, I will show the feasibility to apply this threat to the real-world. To address these problems, I will introduce a principled method to mitigate this threat by exploring the properties of the learning model or the data.

BIOGRAPHY

Chaowei Xiao is an assistant professor at Arizona State University and the research scientist at NVIDIA Research. Dr. Xiao received his B.E. degree in School of Software from Tsinghua University in 2015 and Ph.D. degree in Computer Science Department from University of Michigan, Ann Arbor in 2020, respectively. His research interests lie at the intersection of computer security, privacy, and machine learning. His works have been featured in multiple media outlets, including Wired, Fortune, IEEE SPECTRUM. One of his research outputs is now on display at the Science Museum in London. He has received the best paper award at Mobicom 2014 and ESWN 2021. His group has multiple Ph.D. and internship positions. Feel free to contact him via email (xiaocw@asu.edu).

ENQUIRY

Tel: 3411-2385 Email: comp@comp.hkbu.edu.hk Website: https://www.comp.hkbu.edu.hk/v1/?page=events