香港浸會大學
HONG KONG BAPTIST UNIVERSITY

DEPARTMENT OF
COMPUTER SCIENCE
計算機科學系

ONLINE SEMINAR
2023 SERIES

Department of Computer Science

Mr. Ka Ho Chow

PhD Candidate
Georgia Institute of Technology, USA

Register Now

Date: 17 January 2023 (Tuesday)
Time: 9:15am – 10:15am
Registration: https://bit.ly/cs-ereg

(*Zoom details will only be provided to registrants)

Towards Robust Cognitive Systems: Attacks, Defenses, and Beyond

ABSTRACT

We have witnessed how ransomware attacks compromise critical infrastructures creating chaos in a country, how data breaches cost businesses millions, and how recent cryptojacking attacks degrade system performance. While they continue to roar, new threats are on their way. Machine learning (ML) has created many life-enriching opportunities, but it also introduces new attack surfaces to those cognitive systems. From a security perspective, one could conduct data poisoning during the distributed training phase or generate deceptive queries during the model inference phase to control the behavior of the deployed ML model. From a privacy perspective, adversaries could reconstruct sensitive training data from gradient leakage. These threats hold the potential to create catastrophic consequences and must be thoroughly investigated to design countermeasures. In this talk, I will give an overview of my recent research on analyzing security vulnerabilities and developing mitigation mechanisms for robust computing systems.

BIOGRAPHY

Ka-Ho Chow is a Ph.D. candidate in Computer Science at Georgia Tech under the supervision of Prof. Ling Liu. His research interests lie in strengthening the security, privacy, and performance of data analytics and systems. Ka-Ho's work has appeared at top-tier venues such as SIGKDD, EuroSys, and CVPR. Before joining Georgia Tech, he received his B.Eng. and M.Phil. degrees from HKUST. Ka-Ho is the recipient of the IBM PhD Fellowship 2022, the Croucher Scholarship 2021, the Best Paper Award at ACM EdgeSys 2020, and the Chair's Fellowship 2019 at Georgia Tech.

ENQUIRY

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