Faculty of Engineering
Distinguished Lecture Series

Faculty of Engineering

Cyber Risk Assessment: From Breach Prediction to Incentive Design

Professor Mingyan Liu

Professor of Electrical Engineering and Computer Science
University of Michigan, Ann Arbor

Date : 23 May 2019
Time : 11:00 - 12:00
Venue : Room 801,
Ho Sin Hang Engineering Building, CUHK

Abstract:

In this talk I will present our ongoing effort in the quantitative assessment of an organization's cybersecurity risk from externally observable properties, by applying modern machine techniques to large quantities of Internet measurement data. Specifically, I will first describe the use of host malicious activity data (including spam, phishing, and active scanning) combined with network configuration data to obtain cybersecurity incident prediction at a firm level. I will then briefly describe the additional use of business details about an organization to obtain more fine-grained prediction, which examines not just the overall risk of an incident, but the types of incidents it is particularly susceptible to. Both of these studies follow a supervised learning framework where ground truth information in the form of data breach reports is used. In the third study I will show how deep learning techniques can be used to obtain application-agnostic, universal, and light-weight features from global scan measurements in an unsupervised setting; these features can then be used in a variety of supervised learning applications including that of prediction of malicious hosts. I will conclude the talk by describing how our ability to make predictions, or more generally, our ability to quantify at a global level the security postures of organizations, can be crucial in designing mechanisms to induce more socially desirable behavior at the firm level. In particular, quantitative assessment of this type may be viewed as creating a form of "public monitoring" that enables inter-temporal incentives to sustain long-term security information sharing among firms, or viewed as a form of "security pre-screening" to effectively mitigate moral hazard in underwriting cyber insurance policies through premium discrimination.

Biography:

Mingyan Liu received her Ph.D in electrical engineering from the University of Maryland, College Park, in 2000. She has since been with the Department of Electrical Engineering and Computer Science at the University of Michigan, Ann Arbor, where she is currently a Professor and the Peter and Evelyn Fuss Chair of Electrical and Computer Engineering. Her research interests are in optimal resource allocation, incentive design, and performance modeling and analysis, all within the context of networked systems. Her most recent research activities involve online learning, modeling and mining of large scale Internet measurement data concerning cyber security, and incentive mechanisms for cybersecurity. She is the recipient of the 2002 NSF CAREER Award, the University of Michigan Elizabeth C. Crosby Research Award in 2003 and 2014, the 2010 EECS Department Outstanding Achievement Award, the 2015 College of Engineering Excellence in Education Award, and the 2018 Distinguished University Innovator Award. She holds Best Paper Awards from the International Conference on Information Processing in Sensor Networks (IPSN) in 2012 and the IEEE/ACM International Conference on Data Science and Advanced Analytics (DSAA) in 2014. She has served on the editorial board of IEEE/ACM Trans. Networking, IEEE Trans. Mobile Computing, and ACM Trans. Sensor Networks. She is a Fellow of the IEEE and a member of the ACM.

All are welcome

Host : Professor CHEN Minghua
(Tel: 3943-8452, Email: minghua@ie.cuhk.edu.hk)
Enquiries : Information Engineering Dept., CUHK (Tel.: 3943-8385)
Registration : www.erg.cuhk.edu.hk/erg/Events