Title: Practical Techniques for Privacy-Enhanced Collaborative Filtering

Speaker: Mr Richard Chow
Security and Privacy Researcher and Architect
Intel Corporation

Date/Time: 24 March 2014, 11:00 AM to 12:30 PM
Venue: Video Conference Room, COM1-02-13

Chaired by: Dr Saxena, Prateek, Dean’s Chair Assistant Professor, School of Computing
(prateeks@comp.nus.edu.sg)

Abstract:

Collaborative filtering is a widely-used technique in online services to enhance the accuracy of a recommender system. This technique, however, comes at the cost of users having to reveal their preferences, which has undesirable privacy implications. In this talk we describe two approaches to this problem. In the first, we propose a collaborative filtering system where the system does not observe the users' data and is still able to provide useful recommendations. Our approach involves creating a primitive to cluster similar users privately by modifying existing methods such as Locality Sensitive Hashing. In the second, we propose a technique called differential data analysis to determine which data is important to accuracy of a recommendation algorithm and which is not. We show how this knowledge can be leveraged by existing data obfuscation techniques to provide increased privacy for comparable levels of recommendation accuracy.

Biodata:

Richard Chow is a security and privacy researcher and architect at Intel Corporation. In the past he has held positions as Research Scientist at PARC, Research Scientist at Samsung Electronics R&D, and Security Architect at Yahoo and Motorola. His work concentrates on privacy, big data, mobile, and the cloud. He has over 20 US patents and patent applications and over 25 peer-reviewed journals, conference papers, and book chapters. He was awarded runner-up for the 2010 PET Award for Outstanding Research in Privacy Enhancing Technologies. He has given invited talks at academic conferences and venues such as the RSA Conference and OWASP. He has been invited to serve on numerous Program Committees and has served as Guest Editor of IEEE Security and Privacy Magazine. He has a Ph.D. in mathematics from the University of California at Los Angeles.