Computer Science
Seminar

Differential Privacy: What Does It Mean and What Can Be Achieved?

Dr. Ninghui Li
Purdue University

Abstract: Over the last decade, differential privacy (DP) has emerged as the standard privacy notion for research in privacy-preserving data analysis and publishing. However, there is an ongoing debate about the meaning and value of DP. Some hail that the notion of DP offers strong privacy protection regardless of the adversary's prior knowledge while enabling all kinds of data analysis. Others offer criticisms regarding DP's privacy guarantee and utility limitations.

In this talk, we focus on two issues. One is what does DP mean? More precisely, under what condition(s), the notion of DP delivers the promised privacy guarantee? We show that DP is based on the following Personal Data Principle: "Data privacy means giving an individual control over his or her personal data. Privacy does not mean that no information about the individual is learned, or no harm is done to an individual. Enforcing the latter is infeasible and unreasonable." Furthermore, the question of when DP is adequate is not just a technical question and depends on legal and ethical considerations.

In the second part of the talk, we give a survey of the state of the art in publishing a summary of a relational dataset, ranging from publishing histograms for one-dimensional and two-dimensional datasets, to answering marginal queries for datasets with dozens of dimensions, and finally to finding frequent itemsets in transactional datasets with thousands or more of dimensions.

Brief Bio:

Ninghui Li is a Professor of Computer Science at Purdue University, where he has been a faculty member since 2003. His research interests are in security and privacy. He has published over 130 referred papers in these areas. Prof. Li is current on the editorial boards of Journal of Computer Security (JCS) and ACM Transactions on Internet Technology (TOIT). He was on the editorial board of IEEE Transactions on Dependable and Secure Computing (TDSC) from 2011 to 2015 and the VLDB Journal from 2007 to 2013. He recently served as Program Chair of 2014 and 2015 ACM Conference on Computer and Communications Security (CCS), ACM's flagship conference in the field of security and privacy.

Friday, March 25, 2016, 3:00 pm
Mathematics and Science Center: W301

Mathematics and Computer Science
Emory University