Dissertation Defense

Secure and Privacy-Preserving Distributed Data Release

Slawomir Goryczka
Emory University

Abstract: The rapidly increasing prevalence of distributed data-driven applications has highlighted security and privacy issues in storing and processing sensitive data. Although manipulating raw data may violate privacy of their owners, different techniques of preparing and using privacy-preserving data descriptions can be still used. It remains a challenge, however, to ensure that adapted and new solutions are efficient, secure, and preserve privacy of data owners without disclosing confidentiality of data providers.

The dissertation proposes a new notion of m-privacy that addresses the challenges when data providers may act as adversaries. To verify if such adversaries are capable of breaching privacy, we introduce a few different strategies and an adaptive algorithm to select and run the most efficient approach. In addition, we designed an algorithm to anonymize data, such that its results are m-private, i.e., knowing the results would not help any m colluding parties in their attacks. All verification and anonymization algorithms have been implemented to be run in distributed environments by a trusted third party.

For settings without a trusted third party, we introduce new secure multiparty computation protocols that implement centralized m-privacy verification and anonymization algorithms. For each protocol, we provedits security, analyzed its communication complexity, and evaluated its overall performance for various settings.

The dissertation also describes a new algorithm to build differentially private histograms for records with customized privacy levels. The algorithm has two data partitioning phases (privacy-driven and data-driven). In addition, we adapted a v-optimal partitioning algorithm to be used with differential privacy, and experimentally evaluated their performance.

Finally, the dissertation presents a new differential privacy mechanism that achieves collusion resistance in distributed environments with small overhead. We also defined an enhanced fault tolerant secure scheme (EFT), which can be used to design a variety of secure multiparty aggregation operations, and we employed it to implement our differential privacy mechanism in distributed environments. Both, the privacy mechanism and the EFT scheme have been extensively analyzed and experimentally evaluated.

Tuesday, May 13, 2014, 11:00 am
Mathematics and Science Center: W301

Advisor: Li Xiong

Mathematics and Computer Science
Emory University