Dissertation Defense

Efficient Search and Computation on Encrypted Data with Access Control

Michael Solomon
Emory University

Abstract: Outsourcing data and processing to cloud environments often raises security and privacy concerns, which can be addressed through the use of encryption. But current approaches either provide all-or-nothing encryption, or rely on an omniscient third party to handle granular key management and make access control decisions to provide fine-grained access control, and introduce obstacles to searching over ciphertext. We explore the problem of efficiently searching encrypted data and simultaneously providing embedded fine-grained access control, first in a general setting, and then extended to location-based data. We first propose a new framework for generic database data that enforces access control for queries from different classifications of users, while still providing the capability to search over encrypted data. We then extend our research focus to location-based applications by implementing and assessing several existing location privacy solutions to produce concrete recommendations of the best technique for implementors to choose for specific use cases. And finally, we combine the first and second parts of our work to propose another new framework for mutually private proximity detection (MPPD) to efficiently support searching over encrypted data and enforcing fine-grained access control and privacy for data owners (DO) and users for location-based applications. The culmination of our work provides researchers and application developers with a viable framework that provides MPPD in a categorical setting, and is based on current architectures and technologies.

Tuesday, November 8, 2016, 2:30 pm
Mathematics and Science Center: W306

Advisor: Vaidy Sunderam

Mathematics and Computer Science
Emory University