Ph.D. thesis defense for Kai Zhou

Time: Dec. 15th, 2:15 pm – 4:00 pm

Location: 2555D, Engineering Building

Advisor: Dr. Jian Ren

ABSTRACT

TRADE-OFFS AMONG DATA SECURITY, USABILITY AND COMPLEXITY IN MOBILE CLOUD COMPUTING

Kai Zhou

The proliferation of cloud computing, ubiquitous mobile computing, Internet of Things (IoT) and big data spawns new security and privacy challenges. Big volume of data are produced from ubiquitous mobile devices, aggregated in cloud platforms and transmitted among Internet of Things. The privacy of these user data becomes a great concern. Proper transmission, storing, sharing and utilizing of these data are of great security and performance importance.

Data security, usability and complexity are among the most important design issues in mobile computing environment. Often there are trade-offs among these issues. Data security, as a design goal, is often achieved at the cost of additional computational power. In mobile cloud computing environment, especially for resource-constrained devices, it is critical to achieve certain security requirements without involving too much computation. While data is often encrypted for security purpose in the untrusted cloud environment, the usability of data is often limited. Conventional encryption schemes provide semantic security and allows only users who have the ability to decrypt to utilize the data. However, in many application scenarios, users do not always need to see the data in plaintext in order to fulfill certain functionalities. It is desirable for certain services to be directly conducted on the encrypted data without disclosing the original data. Data usability may decrease as the level of security protection increases, which provides a trade-off between security and usability.

In this dissertation, we primarily focus on designing secure, efficient and versatile protocols achieving the trade-offs among data security, data usability and computational complexity, featuring mobile cloud computing environment. Especially, we focus on alleviating user-side computational overhead for several categories of computational problems, by designing secure outsourcing schemes providing data security and result verifiability. Such problems include general scientific computation and cryptographic computation. We also explore the
trade-off between data security and usability, by designing secure schemes enabling direct utilization of encrypted data. Especially, we proposed a user-centric biometric authentication scheme enabling users to utilize their encrypted biometrics for authentication.

Publication

--- Journal papers ---

1. PassBio: Privacy-Preserving User-Centric Biometric Authentication
   Kai Zhou and Jian Ren
   

2. CASO: Cost-Aware Secure Outsourcing of General Computational Problems
   Kai Zhou and Jian Ren
   

3. P-MOD: Secure Privilege-Based Multilevel Organizational Data-Sharing in Cloud Computing
   Ehab Zaghloul, Kai Zhou and Jian Ren
   

4. Privacy Characterization and Quantification in Data Publishing
   Mohamed Ibrahim, Kai Zhou and Jian Ren
   
   *IEEE Transactions on Knowledge and Data Engineering*, under revision.

   Kai Zhou, H.M. Afifi and Jian Ren
   

6. CDMA System Design and Capacity Analysis under Disguised Jamming
   Tianlong Song, Kai Zhou and Tongtong Li
   

7. Security vs. Usability: Flexible Similarity Queries over Outsourced Encrypted Data
   Kai Zhou and Jian Ren
   
   In preparation.
8. Secure Fine-Grained Access Control of Mobile User Data through Untrusted Cloud
   Kai Zhou and Jian Ren
   
   *The 25th International Conference on Computer Communication and Networks (ICCCN)*, August 1-4, 2016, Waikoloa, Hawaii, USA.

9. Robust CDMA Receiver Design under Disguised Jamming
   Kai Zhou and Jian Ren
   

10. Secure Outsourcing of Scalar Multiplication on Elliptic Curves
    Kai Zhou and Jian Ren
    

11. LinSOS: Secure Outsourcing of Linear Computations Based on Affine Mapping
    Kai Zhou and Jian Ren
    

12. Security and Efficiency Trade-offs for Cloud Computing and Storage
    Jian Li, Kai Zhou and Jian Ren
    