Department of Computer Science
University of Houston

SUMMER 2011 SEMINAR

WHEN: WEDNESDAY, MAY 25, 2011
WHERE: PGH 563
TIME: 11:00 AM

SPEAKER: Dr. Shouhuai Xi, University of Texas at San Antonio

TITLE: Fair and Dynamic Proofs of Retrievability

Abstract:
A specific problem encountered in the context of cloud storage, where clients outsource their data (files) to untrusted cloud servers, is to convince the clients that their data are kept intact at the servers. An important approach to achieving this goal is called Proofs of Retrievability (\POR), by which a storage server can convince a client --- via a concise proof --- that its data can be recovered. However, existing \POR\ solutions can only deal with static data (i.e., data must be fixed), and cannot be used in the setting of dynamic data (i.e., data items need be inserted, deleted, and modified) because of a certain security issue. This motivates us to propose the {\em first} dynamic \POR\ solutions to dealing with dynamic data. Moreover, we introduce a new property, called {\em fairness}, which is inherently important to the setting of dynamic data because, without ensuring it, a dishonest client could legitimately accuse an honest cloud storage server of manipulating its data. Specifically, we present two solutions, one operates in the setting of private verification (i.e., the client itself verifies that its data is secure) and the other operates in the setting of public verification (i.e., a third party verifies that the client's data is secure). Our solutions are based on two new tools, one is an authenticated data structure we call {\em volume 2-3 trees}, and the other is a tailored incremental signature scheme we call {\em hash-compress-sign}. These tools might be of independent value. Finally, we conduct a study with the aim to systemize the knowledge of verifiably secure cloud storage, with emphasis on \POR\ and its sibling solution called Proofs of Data Possession (\PDP), which offers a weaker security guarantee but higher performance.

The talk is based on a joint work with Qingji Zheng.

BIO:
Shouhuai Xu is an associate professor in the Department of Computer Science, University of Texas at San Antonio. His research is primarily in making the cyberspace more secure and trustworthy. He is especially interested in mathematically modeling holistic cyber security and devising practical mechanisms (including provably-secure cryptographic ones) for countering cyber attacks (including botnets). His research has been sponsored by AFOSR, ARO, NSF, and ONR. He earned his PhD in Computer Science from Fudan University. Please refer to www.cs.utsa.edu/~shxu for more information.