

**THE CONCORDIA INSTITUTE FOR INFORMATION SYSTEMS ENGINEERING
IS PLEASED TO PRESENT THE FOLLOWING GUEST LECTURE IN
OUR CIISE SEMINAR SERIES**

Shuai Liu, M.A.Sc.

Concordia Institute for Information Systems Engineering

**Towards Efficient Over-encryption in Outsourced Databases Using
Secret Sharing**

Abstract: Over-encryption is a technique for managing evolving access control requirements in outsourced databases [4]. In over-encryption, a data owner and outsourcing server collectively encrypt resources in such a way that users' accesses can be effectively controlled without the need for shipping the resources back to the owner. One potential limitation of the original over-encryption scheme is that it requires publishing a large amount of tokens. In this paper, we present a new key-assignment approach based on secret sharing. We first give two different key derivation schemes, and then we combine them as one scheme. We analyze the amount of public tokens required by the original over-encryption scheme and our scheme, and we show that our scheme can provide the same over-encryption capability more efficiently.

Biography: Shuai Liu is pursuing her Master of Applied Science in Information Systems Security at Concordia University. Her current main research interest is database security. She received her Bachelor Degree in Information Security from Huazhong University of Science & Technology in China.

Thursday, October 9, 2008

**16:00 – 17:00
EV003.309**

Refreshments will be served

(1515 St. Catherine Street West)