

Concordia Institute for Information Systems Engineering

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

Farkhund Iqbal, Ph.D.

Concordia Institute for Information Systems Engineering

**A Novel Approach of Mining Write-Prints for Authorship Attribution in E-mail
Forensics**

Abstract: Anonymity in e-mail communication is one of the main issues exploited by terrorists, pedophiles, and scammers. Falsifying sender name, address and the path along which an e-mail travels is generally termed as spoofing and forging which can be done even by a novice user. In this context, forensic analysis of e-mails with special focus on authorship attribution can help prosecute the offender of e-mail misuse by means of law. The goal is to determine the likelihood that a specific individual is the author of an anonymous e-mail by examining his/her previously known e-mails. Traditionally, fingerprints are used to uniquely identify individuals during criminal investigations in the courts of law. Analogously, word-print or write-print constituted by using writing style features of an author can be used to discriminate his/her writings from that of others. In current literature, the authorship identification is considered as a text classification problem. Support Vector Machine and Decision Tree are the two commonly employed classification algorithms. Both types of these classifiers suffer from two main limitations: Scalability and interpretability. To address these two shortcomings we have developed a novel approach of authorship attribution in which the unique write-print of every suspect is extracted. These write-prints are used to identify the true author of a disputed e-mail, and to gather convincing and credible evidence to support the finding. To concisely model the write-print of an individual, we borrow the concept of frequent pattern from data mining to capture the combinations of features that frequently occurred in an individual's e-mails.

Biography: Farkhund Iqbal is a PhD candidate in the Faculty of Engineering and Computer Engineering (ENCS), Concordia University, Montreal. His PhD topic is Towards a Framework for E-mail Forensics with special focus on cyber crime investigation, e-mail authorship analysis, e-mail social network analysis and concept analysis. He is an active member of Computer Security Laboratory (CSL) and cyber forensic team at Concordia Institute for Information Systems Engineering (CIISE). The forensic team is working on developing state-of-the-art tools and techniques that would fit an investigator niche.

Thursday, November 27, 2008

**16:00 – 17:00
EV003.309**

**Refreshments will be served
(1515 St. Catherine Street West)**

