Concordia University

Engineering and Computer Science

Concordia Institute for Information Systems Engineering

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

Jeremy Clark, Ph.D
Carleton University

How to "carbon date" digital information

If I claim to have known a message at a certain point in the past, how can you verify this? Time-stamping is one method but it requires you to trust someone to vouch for my claim. In my talk, I will discuss how to put time bounds on the knowledge of a message even if you do not trust anyone. I consider two techniques. Random beacons allow you to determine that a (random) message was known only after a certain point in time in the past, and cryptographic "carbon dating" can establish that a (committed) message was known before a certain time in the past. I will show a practical construction of each, based on financial data and the Bitcoin digital currency respectively. Finally I will consider how these two techniques can be applied to certain types of zero-knowledge proofs (ZKP). The sequential order of the messages in a transcript of a ZKP determines if it is valid or not. Using beacons and carbon-dating, we can construct non-interactive and, with novelty, "short-lived" proofs/signatures whose validity expire after a certain period of time. I will show a few practical applications: verifiable elections and deniable email.

***Biography**:* Jeremy Clark is a postdoctoral fellow working under Paul Van Oorschot at Carleton University. His research interests include authentication protocols for the web, Android and smartphone security, and applied cryptography. Dr. Clark completed his PhD in 2011 at the University of Waterloo. His dissertation was on designing and deploying cryptographically verifiable voting systems including Scantegrity, the first system of this type used in a governmental election. It was awarded the university's gold medal.

Thursday, March 8, 2012 **16:00 – 17:00** **EV001.162**

Université Concordia University