Concordia University
ENCS
Engineering & 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

Mr. Phil Eisen

Cloakware's Core Technology

100 Side Channels and Nothing Worth Watching – Achieving Security in a White-Box World

The introduction of side channel attacks such as power and timing analysis rocked the cryptography world, proving that black-box attack models were unrealistic for smart cards. These days, more crypto than ever before is done in software, where even side-channel attack resistance isn't enough. In this talk, we introduce the white-box attack context, and explain why it is the most realistic model for software security. We will talk about how to create implementations that can achieve some resistance to white-box attacks. We will also discuss approaches to modelling software protection, and ways to measure its effectiveness. Finally, we will discuss open problems (of which there are a ***lot***) in this new and growing field.

Biography: Phil Eisen is the Principal Architect for Cloakware's Core Technology group, which develops Cloakware's flagship software protection product. He was a co-inventor and main developer for Cloakware's first of its kind white-box cryptography solution, which is deployed in well over a billion applications worldwide. Phil holds a BMath and MMath from the University of Waterloo.

Thursday, February 11, 2010

16:00 – 17:00

EV003.309