SCHOOL OF INFORMATICS AND COMPUTING

Informatics Colloquium Series

Douglas Stebila

Friday, February 14, 2014
4:00 pm
Geological Survey (GYS 201)

Provable security of advanced properties of TLS and SSH

Abstract: Cryptographic protocols are fundamental to securing communication on the Internet. The protocols that are used in practice tend to be more complicated than the protocols in academic papers and have more complex security goals. As a result, there has been a significant gap between our mathematical understanding of their security and their real-world security. In this talk, I'll discuss a series of results aimed at reducing this gap.

I'll begin by giving an introduction for non-cryptographers to "provable security", which is the tool we use to formally describe and analyze the security properties of cryptographic schemes. Then I'll discuss two important security properties that have not received a systematic treatment in the cryptographic literature---long-term key reuse and renegotiation---and connect these properties with real-world protocols: the Transport Layer Security (TLS) protocol used to secure billions of transactions on the web and the Secure Shell (SSH) protocol used for remote logins. I'll present security models that better define the properties expected of these complex protocols, and results that demonstrate the conditions under which they have these properties.

This talk covers joint work with Ben Dowling (QUT), and Florian Giesen, Florian Kohlar, and Jörg Schwenk (Ruhr-Universität Bochum).

Short Bio: Dr. Douglas Stebila is a researcher in information security and cryptography at the Queensland University of Technology in Brisbane, Australia. His primary research interest is cryptography, with a focus on the security of Internet and web authentication protocols such as SSL/TLS. He holds an MSc from the University of Oxford and a PhD from the University of Waterloo.

SCHOOL OF INFORMATICS AND COMPUTING
INDIANA UNIVERSITY
Bloomington