Queen's SCHOOL OF Computing

Seminar

CREATE ULSS Distinguished Seminar

Applying Software Protection to White-Box Cryptography

The business world can be a brutal judge of security research ideas. The only thing that matters is the net financial savings of a security technique – does the security technology save more money than it costs? I have been doing research on protecting encryption software, always with an eye on whether it can satisfy business goals. The early days of research into protecting encryption keys in software used a technique called white-box cryptography. The first such methods consisted almost exclusively of look-up tables jammed full of as much math as possible. But these methods have been thoroughly broken. We have been working on different approaches that eliminate tables and rely more heavily on software protection methods. Other topics addressed in this talk at a high level are software security measures and the relationship between white-

Thursday January 14, 2016
2:30pm-3:30pm
Dupuis 217
Light Refreshments

Dr. Michael Wiener
Research and Development
IRDETO
Ottawa ON CANADA

Michael Wiener is a cryptologist who is best known for designing a DES-breaking machine and for attacking RSA with short private exponents. He also co-authored papers on parallel collision search which lead to the best attacks known on many hash functions, elliptic curves, and multiple encryption. He served as Program Chair for Crypto '99 and SAC 2007, and has served on numerous program committees including the first ACM CCS in 1993. He was one of the first employees of Entrust where he specified Entrust's initial PKI architecture. He is now with Irdeto where he leads research and development of advanced white-box cryptography.