Concentration in Information Security

Objective

This concentration is offered as an area of specialization within the Majors or Honours program in computer science. Our main goal is to provide students the best opportunity in Canada to prepare for either a career or graduate school in information security. Students will learn about technological information security threats and controls and higher-level principles guiding their deployment.

Areas covered in this concentration include basics cryptography, theoretical and practical notions of information security, computer network and operating systems security, as well as security threats and controls. This list of topics was developed in conjunction with security experts in local industry, who helped us identify the knowledge base that would most help a new information security professional get started in the field. Some of these areas are covered individually in other Canadian institutions, but this concentration is unique in that it will provide students the most complete and comprehensive computer security background of any educational institute in Canada

For the exact course requirements, students are advised to consult the University calendar. Brief descriptions of the courses that are particularly relevant to the concentration are provided below.

Concentration-Relevant Courses

- CPSC 329 Explorations in Information Security and Privacy
- CPSC 418 Introduction to Cryptography
- CPSC 525 Principles of Computer Security
- CPSC 526 Network Systems Security
- CPSC 527 Computer Viruses and Malware
- CPSC 528 Spam and Spyware
- CPSC 530 Information Theoretic Security
- SENG 521 Reliability and Testing

Description and Rationale

CPSC 329 is a broad survey of topics in information security and privacy, with the purpose of cultivating an appropriate mind set for approaching security and privacy issues. Topics will be motivated by recreational puzzles, possibly stemming from real-life problems, with time allocated for students to attempt to solve these puzzles. Historical background behind the puzzle, together with a technical solution, will be presented afterward. This course is open to all students who have taken a first year programming course.

CPSC 418 provides an introduction to cryptography, with emphasis on attaining well-defined and practical notions of security. The course discusses basic cryptographic primitives, including symmetric and public-key cryptosystems, one-way and trapdoor functions, mechanisms for data integrity, digital signatures, key management, and applications to the design of cryptographic schemes. Assessment will be conducted through homework assignments, exams, and a term paper. Additional application programming exercises may be available for extra credit. Lectures run concurrently with the course PMAT 418 of the same title.

CPSC 525 explores the basic principles of computer security, with emphasis on security policies and protection mechanisms for computing systems. It includes such topics as design principles of protection systems, authentication and authorization, reference monitors, security architecture of popular platforms, formal modeling of protection systems, discretionary access control, safety analysis, information flow control, integrity, role-based access control. The course will introduce legal and ethical considerations as necessary.

CPSC 526 focuses on technical controls designed to provide network security. The course will cover network attacks and ools for detection and protection, such as firewalls, intrusion detection, trusted operating systems, and industrial controls such as SCADA. Other topics include cryptographic protocols for securing IP networks and security for emerging network technologies, such as sensor networks. The course will introduce legal and ethical considerations as necessary.

CPSC 527 instructs students in how insecure software can be exploited to compromise computer systems. As viruses and malware make up the vast majority of network security vulnerabilities, a student specializing in security must understand how they work and how to defend against them.

CPSC 528 investigates spam and other forms of unsolicited bulk electronic communication, and spyware. The course explores spam and spyware countermeasures, and related security problems, legal and ethical issues, and tie-ins to other fields like business and economics.

CPSC 530 explores information theoretic concepts and their applications to cryptography in information theoretic settings. The course discusses formal models of security and efficiency of cryptographic primitives, as well as techniques for analyzing such primitives in these models. Constructions of cryptographic primitives when there is no bound on an adversarys computational resources are also introduced.

SENG 521 teaches principles, processes, and applications of software reliability and software quality assurance. Numerous security problems arise through software vulnerabilities and improper programming practices. Poorly written or unreliable software can pose security threats.

Additional Courses of Potential Interest

- PMAT 419 Information Theory and Error Control Codes
- PMAT 427 Number Theory
- PMAT 429 Cryptography – Design and Analysis of Cryptosystems
- CPSC 519 Introduction to Quantum Computation
- PMAT 527 Computational Number Theory
- PMAT 529 Advanced Cryptography and Cryptanalysis

These courses provide further background in areas related to information security. Any of them would be beneficial to a student taking this concentration. A number of the Pure Mathematics courses constitute a portion of a *Concentration in Cryptogfraphy* that is offered as part of the Bachelor's degree in Pure Mathematics. They provide more in-depth instruction in fields such as theoretical cryptography as well as information and coding theory. Students are advised that these courses have their own pre-requisite requirements.