Canadian Cybersecurity Course Directory

A complimentary guide offered to SERENE-RISC members, collaborators and friends.

Data collected between July and August, 2015

serene·risc

How to use this directory

This is an inventory of courses offered on the topic of cybersecurity by Canadian universities. It is a snapshot taken over July and August 2015; it reflects the information available at that point in time. The courses are listed by province, sorted by university and shown in three categories that reflect broader disciplines: computer science, social science, and law and administration. Where those categories are not shown, all courses at that university are in the field of computer science. For each course, the directory entry includes the course name, department and course code, along with a short description. The information included in this directory is presented in the teaching language of the respective institution.

Please follow up with each university for information on prerequisites, admissions, up-to-date offerings, and schedules.

Alberta

Athabasca University

Computer Science

- Security and Risk Management (Security and Risk Management, ERMS 690)

This course explores the world of technology and information security from a risk management perspective. Through an understanding of history and the examination of trends in today's technology landscape, the course investigates the sources of risk and its business implications.

Law and Administration

- Enterprise Information Security (Computer Science, COMP 660)

In this course, students will study various security issues associated with the development and deployment of information systems, including Internet-based e-commerce, e-business, and e-service systems, as well as the technologies required to develop secure information systems for enterprises. Students will also learn about the policies and regulations essential to the security of enterprise information systems.

- e-Commerce Security, Legal Issues and Ethics (e-Commerce, Business and Administrative Studies, ECOM 425)

e-Commerce Security, Legal Issues, and Ethics is a three-credit, senior-level course that focuses on principles of e-commerce security, law, and ethics from a business perspective. It is aimed at providing you with a broad understanding of the major legal, security, and ethical issues and risks related to e-commerce. Module 1 focuses on security issues and threats pertaining to e-commerce operations. Module 2 addresses the major legal issues related to e-commerce, in particular the challenges in protecting privacy and issues related to intellectual property, consumer protection, international regulations, and cyber torts. The last part of the course focuses on major ethical issues in the information age.

- Issues in Access to Information and Privacy Protection (Legal Studies/Governance/Criminal Justice, LGST 377 and GOVN 377 and CRJS 377)

The proliferation of the internet and other new technologies has had a seismic impact on our ability to create, collect, store and share information. These new communication technologies promise great benefits for the transparency associated with good governance, but also conjure up images of a society where individual privacy is non existent, replaced by the all-knowing, all-seeing "big brother" in either its corporate or governmental versions. LGST 377: Issues in Access to Information and Privacy Protection explores how society grapples with the issues surrounding information access and protection of privacy. It overviews a range of access and privacy debates, including the place of surveillance, anti-terrorism measures, social networking, and the sharing of health information in a free and democratic society. A shortened summary of some of the concerns raised in this course might look like: Internet + biometrics + data mining + RFID technologies = corporate/government "big brother" or

Internet + Freedom of Information (FOI) + social networking = transparency and good governance? Concerns about information access and privacy protection have given rise worldwide to Freedom of Information and Privacy Protection legislation. The course reviews how this legislation can protect and promote societal transparency and privacy, in addition to its conceptual basis.

Concordia University of Edmonton

Computer Science

- Introduction to Computer Security (Computer Science, IT 201)

A review of the major issues of computer security. Classification of security threats; physical security; passwords; encryption; firewalls and routers; security policies; intrusion detection systems; security audits.

- Security Policies, Standards and Management (Information Systems Security Management, ISSM 545)

This course provides students with the standards for creating an enterprise-wide security policy. Topics include: security management principles; defining security requirements; planning and documenting security policies; asset identification and control; system access control; and Internet security. Students also learn how to formulate, administer, manage and evaluate security policies and standards based on best standards for information systems security 'ISO 17799', best practices for security auditing 'COBIT' and the protection of private information required by Canadian laws.

- Digital Forensics (Information Systems Security Management, ISSM 536)

In-depth coverage of live incident response and file system forensic analysis. The course will include the use of various tools and techniques used to extract information from digital media, with a focus on information that is difficult to find using normal methods. These tools and techniques will be supplemented with theoretical discussion, both of the structure of the media itself and of the nature and limitations of digital evidence. The course will cover the most commonly used operating systems and file systems.

- Cryptology and Secure Network Communications (Information Systems Security Management, ISSM 533)

This course in cryptography focuses on securing data through authentication, cryptographic algorithms, access control, public key encryption and public key distribution using best practices for secure communications. Students assess and evaluate cryptographic systems and how they can be incorporated into an information security system and the security plan for the enterprise. Students implement secure sites 'on web servers' that require secure sockets layer for secure transactions. Emerging trends in encryption are discussed to prepare students for the ongoing changes which will be required to keep ahead of hackers. Note: Open only to students in the Master or Diploma of Information Systems Assurance Management program and the Master or Diploma of Information Systems Security Management program.

- Advanced Network Security (Information Systems Security Management, ISSM 531)

Topics will include: intrusion/extrusion detection, network security monitoring, and network event reconstruction. Theory will include problems with and strategies for designing an environment conducive to network monitoring and intrusion detection. Practice will include implementing network security monitoring and intrusion detection in a test environment. Students will gain knowledge and experience identifying, interpreting, and reconstructing intrusions, and other security relevant network events.

- Securing an E-Commerce Infrastructure (Information Systems Security Management, ISSM 525)

Securing the e-commerce infrastructure, taking into account data architecture and management and advanced network protocols. In the e-commerce environment, both information security needs of organizations and privacy needs of customers and clients are examined.

- Operating Systems Security (Information Systems Security Management, ISSM 503)

This course has two components: a theory component to teach the concepts and principles that underlie modern operating systems, and a practice component to relate theoretical principles with operating system implementation. In the theory component, you will learn about processes and processor management, concurrency and synchronization, memory management schemes, file systems and secondary storage management security and protection, etc. The practice component will complement the theory component through some specific assignments illlustrating the use and implementation of these concepts.

Law and Administration

- Governance, Risk and Control (Information Systems Security Management, ISSM 553)

Principles, concepts and techniques applied to information systems security governance, risk and control are explored in this course. Topics covered include: a) the role of governance in the enterprise and study of ISACA's COBIT 5.0 governance framework; b) risk assessment methodologies and tools; and, c) the implementation and management of specific operational IT controls to ensure informational confidentiality, availability and integrity. Through lectures, presentations and labs, students also gain familiarity with issues related to occupational fraud and hacking attempts, and how these threats affect the IT risk management process.

King’s University

- Software Testing and Security (Computing Science, CMPT 405)

This course addresses problems and solutions for long-term software maintenance and evolution, and for large-scale, long-lived software systems. Topics include software engineering techniques for large-scale projects, commercial-grade software testing of complex projects, legacy software systems, software evolution, software maintenance, re-use and programming efficiencies, computer systems and security from a development perspective. The social and professional issues that arise in the context of software engineering will be discussed.

- Introduction to Computer Forensics (Computing Science, CMPT 355)

Introduction to the basics of computer forensics, utilizing analytical and investigative techniques to identify, preserve, extract or collect, examine and interpret stored electronic information.

MacEwan University

- Introduction to Computer Security (Computer Science, CMPT 280)

Students will be introduced to computer and network security and the underlying concepts of confidentiality, integrity, and availability. Topics include common cyberattacks, identifying vulnerabilities and defending against attacks, and approaches to creating secure systems. Students will also work with some of the tools available to security administrators.

Mount Royal University

- Computer Security (Computer Science and Information Systems, COMP 4535)

This course covers the concepts and techniques of computer security. It focuses on security issues relevant to the Internet and protecting an organization's internal network. Risk assessment and development of security policies are covered.

- Network Infrastructure and Security (Computer Science and Information Systems, COMP 3533)

This course covers the principles and practice of computer networking, focusing on the high-level protocol-oriented aspects of computer networks. Networking as it relates to database and file service applications is examined along with Internet structure, protocols and routing. Various aspects of security in networked information systems are studied.

University of Alberta

Computer Science

- Introduction to Discrete Mathematics (Mathematics, MATH 222)

A problem-solving approach to discrete mathematics, covering secret codes, public-key codes, error-correcting codes, enumeration, recurrence relations, induction, graph theory, graph algorithms and parallel algorithms.

- Reliable and Secure Systems Design (Electrical and Computer Engineering, ECE 422)

Causes and consequences of computer system failure. Structure of fault-tolerant computer systems. Methods for protecting software and data against computer failure. Quantification of system reliability. Introduction to formal methods for safety-critical systems. Computer and computer network security.

- Internet Security (Computing Science and Electrical and Computer Engineering, MINT 712)

Security: vulnerabilities of Internet protocols, penetration techniques and defenses, intrusion detection systems. Cryptography: Public and private key cryptography, key negotiation, certificates. E-commerce security standards for both protocols and hosts.

- Codes, Codemakers, Codebreakers: An Introduction to Cryptography (Computing Science, CMPUT 210)

An historical introduction to cryptography intended for a general audience. The development of codes and code-breaking from military espionage in ancient Greece to deciphering hieroglyphics via the Rosetta stone to modern computer ciphers. Includes frequency analysis, one-time-pad security, and public key cryptography.

- Networks and Security (Computing Science, AUCSC 355)

Introduction to computer communication networks and network security. Physical and architectural elements and information layers of a communication network, including communication protocols, network elements, switching and routing, local area networks, and wireless networks. Authentication, cryptography, firewalls, intrusion detection, and communication security, including wireless security.

- Security in a Networked World (Computing Science, CMPUT 333)

Authentication protocols, passwords, shared and public key cryptography, network protocol and network services security, firewalls, malicious code, vulnerability identification, intrusion detection, wireless security.

Law and Administration

- Computer and Information Systems Security (Continuing Studies, EXMGT 5618)

This course will introduce you to information technology security theory and practice. It will give you insight into this critical business area through a review of key information security concepts and the fundamentals of a successful information security program.

- Information Access Applications: Issues and Practices (Continuing Studies, EXIAPP 8176)

Identifies and discusses key access issues and best administrative practices for the successful management and compliance with access to information legislation.

- Privacy in a Liberal Democracy (Continuing Studies, EXIAPP 8173)

Defines and explains the concept of privacy in a liberal democracy. Privacy concepts and principles are explored and discussed through an examination of the Federal Personal Information Protection and Electronic Documents Act (PIPEDA). Key privacy issues facing privacy legislation administrators are also reviewed.

- Privacy Applications: Issues and Practices (Continuing Studies, EXIAPP 8174)

Identify and discuss key privacy issues and best administrative practices for the successful management and compliance with privacy legislation.

- Information Access and Protection of Privacy Foundations (Continuing Studies, EXIAPP 8171)

Provides an introduction to the history, theories, and key concepts relevant for the appropriate administration of access and privacy legislation. Access and privacy concepts and principles are examined using federal, provincial, and municipal legislation.

- Information System Security Management (Management Information Systems, MIS 427)

This course focuses on Information System Security from a Managerial point of view. It examines the IT security needs of all business areas. The course covers aspects of threat assessment, policy creation and enforcement, implementation and the hurdles involved, auditing, and forensics. It also looks at the different ways that compromises can occur and how to detect and prevent them from a planning and Disaster Recovery level. A great many real world examples are used as well as exposing the student to current technology that is used in industry. The main focus is from a manager's point of view and teaches planning skills that are important in a field that grows on a daily basis.

- Health Information Access & Privacy (Continuing Studies, EXIAPP 8177)

Laws governing health information privacy, access, and management have an impact on health care providers, public bodies with a role in the health care sector, employers, professional regulatory bodies, fundraisers, insurers, and researchers. Learn about policies, practices, laws, and regulations that address confidentiality, privacy, and security information. Health Information Protection, addressing Electronic Health Records, E-Health and Telehealth, Health Research, Surveillance, and Public Health and Information Protection issues will also be examined.

University of Calgary

Computer Science

- Spam and Spyware (Computer Science, CPSC 628)

Spam and other unsolicited bulk electronic communication, and spyware. Legal and ethical issues. Countermeasures, and related security problems.

- Cryptography and Number Theory with Applications (Electrical Engineering, ENEL 635)

The topic of the course is to provide the students with vital information about the use of number theory in designing and implementing various public key cryptographic schemes. We will stress on the efficacy of the algorithms used and their application in areas outside cryptography and coding theory.

- Information Theoretic Security (Computer Science, CPSC 630)

Information theoretic concepts such as entropy and mutual information, and their applications to defining and evaluating information security systems including encryption, authentication, secret sharing and secure message transmission.

- Cryptography (Computer Science, CPSC 669)

An overview of the basic techniques in modern cryptography, with emphasis on fit-for-application primitives and protocols. Topics will include symmetric and public-key cryptosystems; digital signatures; elliptic curve cryptography; key management; attack models and well-defined notions of security.

- Network Systems Security (Computer Science, CPSC 626)

Attacks on networked systems, tools and techniques for detection and protection against attacks including firewalls and intrusion detection and protection systems, authentication and identification in distributed systems, cryptographic protocols for IP networks, security protocols for emerging networks and technologies, privacy enhancing communication. Legal and ethical issues will be introduced as necessary.

- Biometric Technologies (Computer Science, CPSC 697)

Principles of biometric system design, technology and performance evaluation. Verification, identification and synthesis in biometrics. Traditional and emerging techniques for fingerprint matching, face recognition, iris modelling, signature authentication, and biometric pattern recognition. Multi-modal biometrics and biometric security.

- Computer Viruses and Malware (Computer Science, CPSC 627)

Study of computer viruses, worms, Trojan horses, and other forms of malicious software. Countermeasures to malicious software. Legal and ethical issues, and some general computer and network security issues.

- Information Security Seminar (Computer Science, CPSC 696)

Topics in information security, such as security management, emerging threats, research frontiers using case studies and best practices.

- Information Theoretic Security (Computer Science, CPSC 530)

Information theoretic concepts such as entropy and mutual information and their applications to defining and evaluating information security systems including encryption, authentication, secret sharing and secure message transmission.

- Spam and Spyware (Computer Science, CPSC 528)

Spam and other unsolicited bulk electronic communication, and spyware. Legal and ethical issues. Countermeasures and related security problems.

- Computer Viruses and Malware (Computer Science, CPSC 527)

Study of computer viruses, worms, Trojan horses, and other forms of malicious software. Countermeasures to malicious software. Legal and ethical issues, and some general computer and network security issues.

- Network Systems Security (Computer Science, CPSC 526)

Attacks on networked systems, tools and techniques for detection and protection against attacks including firewalls and intrusion detection and protection systems, authentication and identification in distributed systems, cryptographic protocols for IP networks, security protocols for emerging networks and technologies, privacy enhancing communication. Legal and ethical issues will be introduced.

- Principles of Computer Security (Computer Science, CPSC 525)

Security policies and protection mechanisms for a computing system, including such topics as design principles of protection systems, authentication and authorization, reference monitors, security architecture of popular platforms, formal modelling of protection systems, discretionary access control, safety analysis, information flow control, integrity, role-based access control. Legal and ethical considerations will be introduced.

- Introduction to Cryptography (Computer Science, CPSC 418)

The basics of cryptography, with emphasis on attaining well-defined and practical notations of security. Symmetric and public key cryptosystems; one-way and trapdoor functions; mechanisms for data integrity; digital signatures; key management; applications to the design of cryptographic systems. In addition to written homework, assessment will involve application programming; additional mathematical theory and proof-oriented exercises will be available for extra credit.

- Explorations in Information Security and Privacy (Computer Science, CPSC 329)

A broad survey of topics in information security and privacy, with the purpose of cultivating an appropriate mindset for approaching security and privacy issues. Topics will be motivated by recreational puzzles. Legal and ethical considerations will be introduced as necessary.

- Principles of Computer Security (Computer Science, CPSC 625)

Security policies and protection mechanisms for a computing system, including such topics as design principles of protection systems, authentication and authorization, reference monitors, security architecture of popular platforms, formal modelling of protection systems, discretionary access control, safety analysis, information flow control, integrity, role-based access control. Legal and ethical considerations will be introduced as necessary.

- Elliptic Curves and Cryptography (Computer Science, CPSC 629)

An introduction to elliptic curves over the rationals and finite fields. The focus is on both theoretical and computational aspects; subjects covered will include the study of endomorphism rings, Weil pairing, torsion points, group structure, and effective implementation of point addition. Applications to cryptography will be discussed, including elliptic curve-based Diffie-Helman key exchange, El Gamal encryption, and digital signatures, as well as the associated computational problems on which their security is based.

Law and Administration

- Security Law (Continuing Education, BMC 236)

This overview of the Canadian legal system emphasizes the legal matters of interest to security personnel. Topics include: the Canadian court system; criminal law and evidence; contract, company and real property law, including the protection of technology and information; labour law and collective bargaining; and laws regulating the security industry.

University of Lethbridge

- Cryptography (Computer Science, CPSC 3730)

Classical ciphers, substitution ciphers, permutation ciphers. Shannon's information theory, entropy, Huffman codes, perfect secrecy and the one-time pad. Symmetric-key ciphers: block and stream ciphers. Public-key cryptosystems. Key distribution. Message authentication and digital signatures.

British Columbia

Kwantlen Polytechnic University

Computer Science

- Security of Wireless Systems (Information Technology, INFO 4370)

Students will learn about wireless security technologies such as advanced user authentication, robust encryption, and intrusion prevention. They also will learn concepts of wireless discovery, wireless attack identification and monitoring, and wireless security policies and solutions. Students will be required to conduct research and work on a project to solve real-world wireless system security problems in a simulated environment.

- Website and Cloud Security (Information Technology, INFO 4125)

Students will learn the core mechanisms and tools for Web and cloud security. They will learn the principles of Web attacks on authentication, users, application servers, data stores, back-end components, application logic and bypassing client side controls. They will learn how to discover and prevent Web security flaws during Web application development and measures to improve Web security. They will also learn how to identify and resolve the security issues specific to public and private clouds.

- Digital Forensics (Information Technology, INFO 4120)

Students will learn the foundations of digital forensics. They will learn the key technical concepts, the methodologies used and the tools needed in digital forensics. Students will learn how to perform examinations for computers, networks, mobile devices, GPS, the Cloud and the Internet. Students will also learn how to collect evidence, document the scenes, and recover deleted data.

- Foundations of Computer Security (Information Technology, INFO 2411)

Students will learn fundamental concepts, theories, methodologies and techniques of computer and network security. Students will gain an understanding of the importance of security within and between organizations, including the ongoing threats and vulnerabilities on networks. In this course the significance of being ethical is emphasized. It covers the aspects of systems security from the perspective of providing security mechanisms for protecting networks. Students will learn several software tools and techniques related to computer security using mechanisms such as cryptographic systems, authentication and access control methods. Different types of network and computer attacks are studied. Tools to discover network designs, functionality, resources and vulnerabilities are introduced.

- Security of Enterprise Networks (Information Technology, INFO 3170)

Students will learn the fundamentals of network security and the principles of firewalls and Virtual Private Networks (VPN). They will learn how to identify network security threats. They will also learn how to select and deploy firewalls and manage VPNs.

Law and Administration

- Cyber Security for Managers (Continuing and Professional Studies, Business, BUSK 9004)

Cyber security issues are all around us and reach nearly every part of our business and work, from online banking and education to Facebook and Wi-Fi. Finally, you can get up to date on Cyber Security basics and fundamentals. Designed for non-technical managers, directors and others in the workplace, you will find out about threats and vulnerabilities, safeguards, common attacks, viruses, malware and spyware, disaster recover planning, intrusion detection/prevention, basic security architecture, introductory forensics, and cyber terrorism. At the of the course you will have the knowledge needed to practice safer computing and safeguard your business and work information.

- Introduction to Security Management (Security Management, SECU 2001)

Students will explore applied ethics and management theory as they relate to security management. They will gain practical knowledge of the practices of security management through case studies, class presentations and guest lectures. Students will apply basic elements of management to practical security industry scenarios. Students will explore topics of particular interest in the industry including confidentiality; liability; employee integrity; human relations; supervision and disciplinary actions; information security; business strategy; and client relations.

Simon Fraser University

Computer Science

- Cryptography (Mathematics and Computing Science/Mathematics, MACM 442 and MATH 742)

An introduction to the subject of modern cryptography. Classical methods for cryptography and how to break them, the data encryption standard (DES), the advanced encryption standard (AES), the RSA and ElGammal public key cryptosystems, digital signatures, secure hash functions and pseudo-random number generation. Algorithms for computing with long integers including the use of probabilistic algorithms.

- Cryptography and Cryptographic Protocols (Computing Science, CMPT 404)

The main cryptographic tools and primitives, their use in cryptographic applications; security and weaknesses of the current protocols. The notion of security, standard encryption schemes, digital signatures, zero-knowledge, selected other topics.

- Data Management and IS Audit (Business Administration, BUS 464)

Focuses on the use of integrated database management systems in organizations and their application to IS audit and security. Students analyze data models and create business reports based on SQL. SQL queries are designed for audit and information security purposes. The CoBIT framework is used to understand foundations of IS audit.

Social Science

- Computer Forensics and Cybercrime (School of Criminology, CRIM 480)

Advanced exploration of high-tech crime and exploration of the tools and techniques used by cyber-criminals. Examines the techniques used by law enforcement to investigate and prosecute offenders, as well as the probable future development of cybercrime.

- Advanced Issues in Cybercrime (School of Criminology, CRIM 481)

Analysis of complex, emerging and current cyber-security threats. Discusses methods used to identify cybercrime threats and vulnerabilities, as well as the social, economic and legal implications. Insight into creating an effective defensive plan, and an understanding of future security trends and threats which are likely to develop.

Law and Administration

- Introduction to Cybercrime (School of Criminology, CRIM 380)

Explores legal, technical and social issues in cybercrime. Discusses the nature of cybercrime, with specific examples, and methods of regulation in Canada and worldwide. Addresses origins and extent of cybercrime, responses from the legal system and consideration of the wider effects for society.

Thompson Rivers University

Computer Science

- Introduction to Computer Security (Computing Science, COMP 2730)

This is an introductory course on computer and information system security. Students discuss key security requirements such as Confidentiality, Integrity, and Availability (CIA), and the mechanisms used to ensure them, such as Authentication, Access Control, and Auditing (triple-A). The course lays the foundation for further study, and for students seeking industry certifications, such as CompTIA Security+ or CISSP.

- Network Security (Computing Science, COMP 3260)

Most applications on the Internet exchange information between clients and servers. The exchange of information over the Internet is very challenging due to an abundance of different technologies, and all the security issues that arise between those technologies. Students explore the Internet network model and architecture, network protocol issues, the security issues on the Internet, malicious software, and finally how to protect systems and LANs.

- IT Security (Computing Science, CMPT 4259)

This course provides the background to evaluate the risks and assess the available tools to ensure a secure environment for the IT infrastructure of an organization. Security issues and solutions are discussed from a management and a technical perspective. Students learn about security policies, procedures and user awareness as well as disaster recovery and business continuation planning. Case studies and self-assessment exercises provide for self-evaluation, reinforcing the concepts presented in the course. Upon completion, students will understand the security threat and the risk assessment process and how to apply it to operating systems and network communications security in a way that supports business requirements.

- Digital Identity Management: Concepts and Technologies (Computing Science, CMPT 4619)

In today's online world, enterprises are under increasing pressure to integrate a variety of business processes with their networked systems to make them more secure, accessible and user-friendly. Enterprises are finding that the management of user identity is key in connecting employees, customers, suppliers and partners both inside and outside organizational networks. This seminar provides students with an understanding of the concepts and technologies related to building an effective enterprise identity management architecture. Students examine the concepts, tools, and technologies that allows enterprises to build an identity management architecture that achieves business process goals on a foundation of managed digital identity. It also investigates the intersection between corporate and public worlds of online identity, thus providing an opportunity to look at the way living online is fundamentally changing how communities of trust are developed.

Social Science

- Computer Forensics and Cybercrime (Criminology, CRIM 4809)

This course provides an advanced exploration of high tech crime in addition to the tools and techniques used by cyber-criminals. Techniques used by law enforcement to investigate and prosecute offenders as well as the probable future development of cybercrime are topics that are examined.

Law and Administration

- Introduction to Cybercrime (Criminology, CRIM 3809)

This course explores legal, technical and social issues in cybercrime. It discusses the nature of cybercrime, with specific examples and methods of regulation in Canada and worldwide. Addresses origins and extent of cybercrime, responses from the legal system and consideration of the wider effects for society.

- Information Security Management for Business (Management Information Systems, MIST 4620)

Students develop a general understanding of information technology security. Dependency on computer technology and the Internet has grown to a level where all organizations must devote considerable resources to managing threats to the security of their mobile, desktop and networked computer systems. Topics include introduction to information security; basic need for security; legal, ethical, and professional issues; risk management; information security policies and procedures; information security planning; access control systems and methodology; principles of cryptography; and operations security.

University of British Columbia

Computer Science

- Introduction to Computer Security (Electrical and Computer Engineering, CPEN 442 and EECE 412)

Security risks, threats, and vulnerabilities from technical perspectives; confidentiality, integrity, and hybrid policies; cryptography, access control, assurance, accountability, and engineering of secure systems.

- Network Systems and Security Professional (Continuing Studies, -)

Skills in network systems and security administration are in high demand. The UBC Certificate in Network Systems and Security Professional (NSSP) program was developed in close collaboration with leading technology companies to ensure that only relevant skills and technologies are addressed. The result is a streamlined yet comprehensive program that ensures you are well prepared for a successful career in computer network administration, network management and network security with job-ready knowledge and skills, and exposure to the latest technologies.

- Securing an Online Enterprise (Continuing Studies, IB 400)

As infrastructure security becomes crucial to today's organizations, companies must implement policies and processes to secure their business and intellectual properties. In this 100% online course, you learn how to secure an online enterprise through a story-centred curriculum, in which you complete tasks and objectives that build on an actual workplace project. Gain the knowledge and skills to identify and respond to a security incident in a timely manner; properly secure the server and network; develop a robust incident response plan and security policy; and create a baseline for training employees on their role in company security. You will be able to enact an end-to-end response plan in a short window of time, while keeping the business needs in the forefront. This course is suited to system or network administrators with some infrastructure experience but no or little security training. The Story-Centred Curriculum provides a rich, engaging story that is closely analogous to situations the student experiences or will soon experience in their real-world work. The students play an important role in the story, where they work to achieve one or more significant objectives over a series of tasks. The roles are those that the graduate of such a course might actually take on in real life. Students, usually working in teams, are given detailed information about the simulated company they are working for and are assigned complex, realistic projects. Supporting materials and resources are provided online, and expert mentors are available to answer questions and point students in the right direction on an as-needed basis. There are no lectures or tests, students learn by doing, and acquiring knowledge and skills as they progress through the course. As infrastructure security becomes crucial to today's organizations, companies must implement policies and processes to secure their business and intellectual properties. In this 100% online course, you learn how to secure an online enterprise through a story-centred curriculum, in which you complete tasks and objectives that build on an actual workplace project. Gain the knowledge and skills to identify and respond to a security incident in a timely manner; properly secure the server and network; develop a robust incident response plan and security policy; and create a baseline for training employees on their role in company security. You will be able to enact an end-to-end response plan in a short window of time, while keeping the business needs in the forefront. This course is suited to system or network administrators with some infrastructure experience but no or little security training.

- Computer and Information System Security (Computing Information and Cognitive Systems, CICS 518)

Technical, operational, and managerial issues of computer system security, computer security threats, techniques for detecting and preventing security violations, instituting safeguards, and applying appropriate levels of security for the perceived risk.

Law and Administration

- Digital IP and Rights Management (Continuing Studies, IZ 109)

Unlimited online access has opened up a space that is open-sourced, user-generated and user-controlled. Understanding the underlying principles of digital intellectual property is critical to any communications plan. Learn to determine who owns rights to digital content and discover both the opportunities and risks with the transfer of information. What are the limits to curating digital content when producing, borrowing or sharing in a public or private space? What constitutes piracy? Learn when to pay proper attribution, what creative commons means, and when copyright law is applied. Ensure your digital communications can evolve along with them and reinvent itself on each device and platform.

University of Northern British Columbia

Computer Science

- Internet and Mobile Security (Mathematical, Computer, Physical, and Molecular Sciences, CPSC 744-3)

This course provides a comprehensive study of issues in internet and mobile security including types of security services, firewalls and virtual private networks. Other topics covered include denial of service attacks, virus, worms, Trojan horses, replay violations, cookies, Public key cryptography, hash algorithms, Data Encryption Standard (DES), MD5, Modular arithmetic, primes and Euclid's algorithm, Public key algorithms, Prominent Internet Security, Procedures like Diffi e-Hellman, authentication, passwords, mutual authentication, authorization, RADIUS and AAA, IPsec, IKE, PKI. The course also covers transport layer security and secure socket layer protocols, authentication of mobile users and privacy operations.

- Cryptography and Data Security (Computer Science, CPCS 346-3)

This course is an introduction to the basic algorithms for confidentiality and authenticity of data. Topics include cryptographic primitives and specific realizations, transposition and substitution ciphers, modern private and public key encryption systems, digital signature, realization of AES, DES, RSA, and other systems.

Social Science

- Intelligence and Security (Global and International Studies, INTS 378-3)

Intelligence-gathering is a significant, and in the case of spying, covert aspect of global society. This course is a comparative analysis of the place of security and intelligence in global affairs. The role of the four major elements of intelligence (collection, counterintelligence, analysis and estimates, and covert action) are examined as are the oversight and control issues raised by these activities.

University of the Fraser Valley

- Advanced Topics in Information Security (Computer Information Systems, CIS 497)

This advanced topics course is designed to provide study of the latest up-to-date technologies and issues in information security not covered in other courses. Topics may be drawn from areas such as physical and network security, secure programming, policies and ethics, intrusion detection, OS hardening, cryptography, cultural issues, forensic issues and others. Topics will vary depending on semester and instructor. Students should consult the department for current offerings.

- Malicious Software and Attack Prevention (Computer Information Systems, CIS 325)

This course will provide students with proven techniques for allowing authorized users access to the Internet while protecting the inner network from attack by someone who has circumvented the outer defence or from internal attack. Methods and technologies such as secure programming, viruses, host-based intrusion detection, auditing, threat modeling, forensics, software firewalls, and operating system hardening will be discussed.

- Networking Security Architecture (Computer Information Systems, CIS 321)

This course focuses on network security architectures, procedures, and processes. Practical hands-on skill development is provided in security system technologies, security policy design, firewall design and implementation, router security architectures, authentication and authorization systems, Intrusion detection, and VPNs. This course will include the "Cisco – Fundamentals of Network Security" learning objectives.

- Network Security and Cryptography (Computing Science, COMP 490)

This course will cover important concepts in conventional encryption algorithms such as AES, public-key design and algorithms such as RSA and elliptic curve, digital signatures and authentication protocols such as Kerberos, and key managements such as PKI and X.509.

- Principles of Information Systems Security (Computer Information Systems, CIS 221)

This course provides an introduction to proven techniques for protecting information systems from intruders, while allowing the required access to authorized users. This course is introductory and is designed to provide an overall view of security in the modern information world. Several hands-on lab projects will be completed using Linux- and/or Windows-based computer systems.

University of Victoria

Computer Science

- Cryptography (Computer Science, CSC 529)

Paradigms and principles of modern cryptography. Topics include: review of classical and information-theoretic cryptography; block ciphers; DES, Cryptanalysis of DES, modes of operation, AES; Cryptographic hash functions and message authentication codes; public key cryptography, RSA, ElGamal and other public key systems, signature schemes; introduction to security protocols; secret sharing schemes and zero knowledge techniques.

- Digital Identity Management (Computing and Technology, TETS 461)

While the notion of identities in the physical world is fairly well understood, as technology evolves so too do the ways people identify themselves online. This makes digital identity management a growing concern for businesses, governments and IT professionals. Our new online course, delivered in 7 sessions, will help you navigate the complexities of online information security, position you at the forefront of technological change and shape your potential for career growth.

- Computer Forensics Methodologies (Electrical Engineering, ELEC 570)

Digital forensics notions and techniques used in the investigation of cybercrimes. Legal awareness of computer security and forensics, evidentiary process techniques, computer forensics methodologies with an emphasis on computer incident response and Information Technology (IT) systems' protection. Ethics, rules of evidence, effective communications, search and seizure relative to privacy legislation. Threats, how they can be detected, and controls to reduce the likelihood of their occurrence.

- Security, Privacy, and Data Analytics (Electrical Engineering, ELEC 572)

Explores the underlying theoretical foundations of information security and privacy issues from an engineering perspective. Applications of information-theoretic concepts, techniques, and methods to the problem of quantifying achieved levels of security and privacy in larger-scale systems in the presence of adversaries.

- Advanced Network Security (Electrical Engineering, ELEC 567)

Presents, from a practical perspective, underlying principles and techniques of network security. Students will be exposed to ethical hacking, and penetration testing. Various protection methods, used in practice to detect and respond to malicious network attacks, will be presented. Students will also learn how to implement successful security policies and defense mechanisms and strategies, with a particular focus on firewalls, intrusion detection and response, virtual private networks, and biometrics technologies.

- IT Security (Computing and Technology, TECJ 425)

This course provides you with the background to evaluate the risks and assess the available tools to provide a secure environment for the IT infrastructure of an organization. Security issues and solutions are discussed both from a management and a technical perspective. Upon completion of IT Security, you will understand the security threat and the risk assessment process and how to apply it to operating system and network communications security in a way that supports business requirements. In addition, you will learn about security policies, procedures and user awareness, as well as disaster recovery and business continuation planning. Case studies and self-assessment exercises provide for self-evaluation, reinforcing the concepts presented in the course.

- Network Security (Software Engineering, SENG 461)

Surveys the challenges, principles and practice of modern network security. Topics covered include network security vulnerabilities and threats; network security risk analysis techniques and countermeasures; design and implementation of secure network architecture; intrusion detection and prevention models and technologies; firewall architectures and technologies; network security protocols; Virtual Private Networks (VPNs); principles, techniques and practice of network forensics.

- Cryptography (Computer Science, CSC 429 and CSC 529)

Fundamentals of modern cryptography. Topics include: review of classical and information-theoretic cryptography; block ciphers, DES, cryptanalysis of DES, modes of operation, AES; cryptographic hash functions and message authentication codes; public key cryptography, RSA, ElGamal and other public key systems, signature

- Hardware Security (Electrical Engineering, ELEC 548 and CENG 448)

Introduction to abstract algebra and finite field arithmetic. Hardware attacks and mitigation techniques. Hardware trojans and hardware trojan detection techniques. Trusted design in FPGAs. Security in embedded systems. Design for hardware trust. Security and testing. Students will be required to complete a project.

- Security, Privacy and You (Engineering, ENGR 100)

A non-specialist tailored introduction to cyber-security and cyber-privacy issues within modern societies. Topics to be covered include: basic privacy issues within social networking, mobile location aware services, and the legal and regulatory frameworks governing privacy in Canada; cyber-security approaches in eCommerce, web sites, electronic banking, and mobile devices; common methods of attack; and basic cyber-defense methods and privacy preserving measures. Underlying technologies will be discussed as required but at levels suitable for non-specialists.

- Security Engineering (Software Engineering, SENG 360)

Topics include basic cryptography, security protocols, access control, multilevel security, physical and environmental security, network security, application security, e-services security, human aspects and business continuity planning. Discusses applications which need various combinations of confidentiality, availability, integrity and covertness properties; mechanisms to incorporate and test these properties in systems. Policy and legal issues are also covered.

- Cryptography (Computer Science, CSC 529)

Paradigms and principles of modern cryptography. Topics include: review of classical and information-theoretic cryptography; block ciphers; DES, Cryptanalysis of DES, modes of operation, AES; Cryptographic hash functions and message authentication codes; public key cryptography, RSA, EIGamal and other public key systems, signature schemes; introduction to security protocols; secret sharing schemes and zero knowledge techniques.

- Cryptography (Computer Science, CSC 429)

Fundamentals of modern cryptography. Topics include: review of classical and information-theoretic cryptography; block ciphers, DES, cryptanalysis of DES, modes of operation, AES; cryptographic hash functions and message authentication codes; public key cryptography, RSA, EIGamal and other public key systems, signature schemes; introduction to security protocols.

- Practice of Information Security and Privacy (Software Engineering, SENG 460 and ELEC 574)

Aims to present a holistic view of various security engineering topics through practical case studies. Topics include enterprise security architecture, security threat and risk assessment, education and awareness, monitoring, investigation and forensics, application security, media handling and intellectual property, privacy, physical and environmental security, and business continuity planning. Also introduces information security-related certification and relevant professional associations.

Social Science

- White-Collar Crime (Sociology, SOCI 312)

An examination of the neglected problem of white-collar crime. Topics include corporate crime, financial fraud, occupational crime, cybercrime, worker safety, environmental crime, consumer victimization, professional misconduct, and the corruption of science.

Law and Administration

- IT Security (Centre for Continuing Education, -)

This course provides you with the background to evaluate the risks and assess the available tools to provide a secure environment for the IT infrastructure of an organization. Security issues and solutions are discussed both from a management and a technical perspective. Upon completion of IT Security, you will understand the security threat and the risk assessment process and how to apply it to operating system and network communications security in a way that supports business requirements. In addition, you will learn about security policies, procedures and user awareness, as well as disaster recovery and business continuation planning. Case studies and self-assessment exercises provide for self-evaluation, reinforcing the concepts presented in the course.

- How an IT Security Program Will Help Your Organization (Centre for Continuing Education, -)

This seminar is about developing an IT security program that supports your organization and business objectives. The IT security program encompasses all the services and activities that the IT security person, or team, delivers. Without adequate oversight and governance the IT security activities will not align correctly with organization and business requirements. The security function will drift around depending on the wind of the day. A good solution is to run IT security within or through an IT security program approach.

Vancouver Island University

Computer Science

- Information Technology Security (Trades & Applied Technology, ITAS 218)

This course introduces students to the essential concepts surrounding information technology security. Topics include operating system and network vulnerabilities, web application security, cryptography, password management and access control, as well as business-related topics such as disaster recovery and risk management.

Law and Administration

- Forensic Accounting and Data Analysis (Business and Management, FORE 410)

An in-depth look at investigative accounting and data analysis. Topics include expert independence, rules of documentary evidence, financial interviewing, report writing, forensic accounting strategies, and the ACFI code of ethics and professional standards.

- Forensic Investigation - an Integrated Case (Business and Management, FORE 490)

The Forensic Accounting and Fraud Investigation capstone course. Students complete a forensic consultation practice set including a letter of engagement, investigation, preparation for expert witness court testimony, and, through creating an organizational culture of compliance, recommendations to the client on fraud prevention.

- Forensic Investigations and Asset Recovery (Business and Management, FORE 350)

An exploration of the processes for forensic investigation and asset recovery. Topics include planning an investigation, the analysis cycle, computer assisted and internet investigations, interviewing, report writing and evidence preparation, strategies supporting legal action, asset tracing and recovery, and handling and processing forensic documents.

- Accounting and Finance for Fraud Investigators (Business and Management, FORE 310)

An overview of accounting and finance for forensic accountants, investigators, and other professionals. Topics include finance, business, internal controls and organizational systems for fraud investigators, red flags and financial statement analysis.

- Fraud and Commercial Crime (Business and Management, FORE 300)

An overview of fraud and commercial crime for forensic accountants, investigators, and other professionals. Topics include commercial crime, business fraud prevention and detection, fraud psychology, vulnerability, characteristics and red flags of fraud, forensic investigation professionals, standards and ethical codes.

- Fraud, Commercial Crime and Evidence (Business and Management, LAWW 348)

An overview of the Canadian legal system pertaining to fraud. Topics include civil and criminal fraud laws, rules of evidence, evidence preparation for civil and criminal cases, and the responsibilities of the expert witness

Manitoba

Brandon University

- Cryptography and Number Theory with Applications (Mathematics & Computer Science, 62:265)

An introduction to Number Theory and its application to cryptography. The topics in number theory include congruences, residues, Fermat's Theorem, Chinese Remainder Theorem, primality tests, and Galois Fields. Some simple ciphers and their history will be discussed followed by a careful study of currently employed protocols and standards such as Diffie-Hellman, elgamal, RSA, ECC, and AES. If time permits more experimental topics such as Quantom and Algebraic Cryptography, and zero knowledge proofs will be introduced.

Université de Saint-Boniface

- Sécurité informatique (Informatique, IG 213)

Principes de sécurité des systèmes informatiques. Les divers concepts, théories et définitions de la sécurité. Quelques connaissances pratiques sur la sécurité des systèmes informatiques.

University of Manitoba

- Introduction to Cryptography and Cryptosystems (Computer Science, COMP 4140)

Description and analysis of cryptographic methods used in the authentication and protection of data. Classical cryptosystems and cryptoanalysis, the Advanced Data Encryption Standard (ADES) and Public-key cryptosystems.

- Computer Security (Computer Science, COMP 4580)

Computer security and information management. This course will examine state-of-the-art knowledge about the issues relevant to data and computer security.

University of Winnipeg

- Cisco CCNA Security (Professional, Applied and Continuing Education, DIT 33004)

The student will be introduced to the methodology surrounding incident response (IR), response escalation, and vulnerability analysis (VA). The course will cover the processes and procedures involved with IR and VA, and provide students with limited practical analysis training related to response escalation.

- Implementing Security (Professional, Applied and Continuing Education, DIT 16034)

This course introduces the more technical aspects of security. Building on the concepts covered in Network Security 1, students will learn about practical topics such as Firewalls, Intrusion Detection, and Cryptography. Further to this, they will explore the anatomy of an attack, analyze how many types of electronic attacks function, and how they can be prevented. This course provides the grounding in common technical aspects of Network Security. The students know the theory as a result of the first level, and will learn how to apply those tools and concepts to real-world solutions.

- Vulnerability Analysis (Professional, Applied and Continuing Education, DIT 36063)

The student will be introduced to the methodology surrounding incident response (IR), response escalation, and vulnerability analysis (VA). The course will cover the processes and procedures involved with IR and VA, and provide students with limited practical analysis training related to response escalation.

- Web Security (Professional, Applied and Continuing Education, DIT 36067)

As more of our world becomes integrated with technology, the risks of cybersecurity become an increasing concern to all businesses. This course provides a theoretical and practical framework for web application security and explores the processes that organizations can develop to guard against network intrusions. On successful completion of this course, students will gain an understanding of how to pinpoint potential security threats and to protect networked information from hackers trying to penetrate network vulnerabilities. Topics will include intrusion detection, network controls, defence tools and techniques, privacy protocols, access controls, and computer forensics.

- Cisco CCNA Ethical Hacking (Professional, Applied and Continuing Education, DIT 33001)

"Ethical hacking" is defined as the use of hacking skills for defensive purposes. Hackers want to know how things work and are always taking a critical view about what they learn. Ethical hacking is about doing this with a defensive mindset and is not just about attacking. Ethical hackers put their outcomes to good use and help improve security in the process. Ethical hacking develops your critical thinking and troubleshooting skills and requires a willingness to look at technology from unusual perspectives. Experimentation is critical. The objectives of ethical hacking are not to cause mischief or to seize control of what does not belongs to us. Rather the objectives are to look for ways to protect organizations' assets and facilitate improvements.

- Computer Forensics (Professional, Applied and Continuing Education, DIT 33003)

The purpose of this course is to introduce students to digital forensics techniques, tools and scenarios. In this course, students are exposed to basic concepts such as evidence acquisition, processing and retention, Canadian and American legislation issues regarding digital forensics. The course is designed to be conceptual in nature and provides limited hands on experience in working with many of the concepts presented.

- Information Assurance and Security Level 3: Safeguards and Countermeasures (Professional, Applied and Continuing Education, DIT 15537)

Given the vulnerable nature of cybersecurity, threat management is the life vein of our global enterprise system. This course is the third level of a series of four courses in information assurance and security and introduces students to the concepts of safeguards and counter measures. Topics will include remote access controls, firewalls, intrusion detection systems, and virtual private networks. The course is more conceptual in nature and provides some hands-on experience.

- Information Assurance and Security Level 2: Cryptography and Encryption (Professional, Applied and Continuing Education, DIT 15536)

The purpose of this course is to introduce students to the areas of Cryptography and Encryption information security. The course provides the conceptual foundation for more advanced topics covered in later Information Assurance and Security courses. In this course, students are exposed to basic concepts such as how encryption started, advances, threats, procedures and security management issues. The course is designed to be conceptual in nature and provides limited hands on experience in working with many of the concepts presented.

- Information Assurance and Security Level 1: Information Security Management (Professional, Applied and Continuing Education, DIT 15535)

The purpose of this course is to introduce students to the area of network and information security. This course builds the conceptual foundation for the advanced Information Assurance and Security (IAS) courses. Topics include the context of information security, legislation, threats, policies, procedures, security management issues, and risk management and assessment. This course is more conceptual in nature and provides limited hands-on experience in working with many of the concepts presented.

- Theory and Practice of Security and Privacy (Applied Computer Science and Society, GACS 7104)

This course provides students an understanding of theoretical and practical aspects of security and privacy and opens them up to the current research challenges in this area. Topics include classical cryptography, symmetric encryption, public key cryptography, key distribution mechanisms, digital signature, entity and message authentication, access control, multimedia security and digital right management, secret sharing, physical security, privacy preserving techniques such as data aggregation, perturbation, k-anonymity and l-diversity.

- Computer Security and Privacy (Applied Computer Science, ACS 3921 and 4921)

This course introduces students to the security and privacy issues in computer systems. It covers the fundamental computer security techniques such as encryption methods, public key cryptography, hash function and signature schemes, key exchange protocols, authentication and access control models. The course also examines the applications of these techniques for multimedia security, intrusion detection, copyright and password protection, and protection from malicious programs. Privacy preserving techniques such as data aggregation, perturbation, k-anonymity and l-diversity, and ethical issues are also discussed. Students at the 4921 level additionally undertake a comprehensive project on a topic related to computer security and privacy.

- Information Assurance and Security Level 4: Incident Response (Professional, Applied and Continuing Education, DIT 15914)

While predictability is somewhat elusive in the cybersecurity realm, predictability measures are essential to incident response systems. This course introduces students to best practice approaches and methodologies for managing incident response (IR), response escalation, and forensic evidence collection. This is the final course in a series of four courses in the area of Information Assurance and Security. The course will cover the processes and procedures involved with incident response (IR) and provide students with practical hands-on training related to response escalation and forensic evidence gathering.

New Brunswick

Mount Allison University

- Cryptography (Computer Science, COMP 4651 and MATH 4651)

This course is an introduction to cryptographic algorithms and to the cryptanalysis of these algorithms, with an emphasis on the fundamental principles of information security. Topics include: classical cryptosystems, modern block and stream ciphers, public-key ciphers, digital signatures, hash functions, key distribution and agreement.

Université de Moncton

Computer Science

- Sécurité informatique (Sciences, INFO 4029)

Définitions formelles des concepts de sécurité informatique, confidentialité et intégrité des données. Évaluation et gestion des risques de sécurité. Éléments de cryptographie. Méthodes d'authentification. Virus. Bombes logiques. Aspects légaux. Contrôle d'accès aux bases de données. Noyau de sécurité. Méthodes de vérification. Sécurité sur l'Internet et les Intranets.

Law and Administration

- Droit de l'information (Droit, DROI 3542)

Étude des problèmes juridiques liés à l'émergence des nouvelles technologies se rapportant au droit de l'internet, au droit du divertissement, des télécommunications et des médias, de la diffamation, du commerce électronique, au droit de l'accès à l'information ainsi qu'à la protection des données et de la vie privée.

University of New Brunswick

Computer Science

- Cryptanalysis and Database Security (Computer Science, CS 6355)

This course is a practical survey of the principles and practice of information security. Topics include conventional encryption, asymmetric and symmetric cryptology, digital signatures, key exchange, authentication, viruses, worms, electronic mail security, network management security, the common criteria, and threat risk management.

- Information Security (Information Systems, INFO 2403)

This course is an introduction to information security. Topics normally covered include: Critical infrastructures Protection, the Corporate Security Policy, Threat Risk Assessment, Security Models, Mandatory and Discretionary Access Control, Symmetric and Asymmetric Cryptography, Message Authentication, Message Digests, Public Key Infrastructure.

Law and Administration

- Cyber Security for Managers (College of Extended Learning, -)

Cyber security issues are all around us and reach nearly every part of our business and work, from online banking and education to Facebook and Wi-Fi. Finally, you can get up to date on Cyber Security basics and fundamentals. Designed for non-technical managers, directors and others in the work place, you will find out about threats and vulnerabilities, safeguards, common attacks, viruses, malware and spyware, disaster recover planning, Intrusion Detection/Prevention, basic security architecture, introductory forensics, and cyber terrorism. At the end of this course, you will have the knowledge needed to practice safer computing and safeguard your business and work information.

- Technology, Security and Risk (Business Administration, ADM 4718)

Examines security and risk from a broad perspective. Topics covered include computer security, physical security of premises, shoplifting, corporate intelligence, corporate espionage, and issues of broad social importance such as airline security and terrorism.

- Threats, Risks and Opportunities: Developing a Cyber Security Strategy for your Organization (College of Extended Learning, CMPW 7802)

Join UNB's David Shipley, director of strategic initiatives for an afternoon focused on understanding the cyber security threats facing your organization and how your team can develop and implement plans, processes and technologies to defend against an increasingly dangerous online environment.

- Legal, Privacy, and Security Issues in Electronic Commerce (Business Administration, BA 3718)

This course deals with the various systems that provide privacy and security on the Internet, as well as the legal issues that arise in electronic commerce. Includes an examination of encryption, fire walls, user authentication, as well as copyright of intellectual property and contracts.

Newfoundland

Memorial University

- Computer and Communciations Security (Engineering and Applied Science, ENGI 8868)

examines the techniques used to provide security in communication networks and computer systems. The course focuses on topics in cryptography required to provide privacy, authentication, and integrity, including symmetric key ciphers, public key ciphers, message authentication, and digital signature schemes.

- Information Security, Privacy, and Ethics (Business Administration, BUSI 5703)

examines the use of information technology and related privacy, security, and ethical issues in the information age. Topics covered will include information and property rights and obligations; system quality; quality of life; accountability and system controls; behavioural factors that can lead to data loss; legal issues; and managerial responsibilities. The course examines these topics from individual, society, and business perspectives.

Nova Scotia

Acadia University

Computer Science

- Topics: Computer and Network Security (Computer Science, COMP 4443)

This course will cover selected topics such as: authentication applications, data integrity and privacy, anonymity, security infrastructures and intrusion prevention, network attacks, and wireless Networks and Security.

- Cryptography (Mathematics and Statistics, MATH 4333)

This course is an introduction to modern cryptographic techniques and their mathematical foundations. Review of elementary number theory and algebra; classical cryptosystems; encryption standards; public key cryptosystems; digital signatures. Elliptic curve cryptography and quantum cryptography may be included.

- Security (Computer Science, COMP 2523)

Topics include cryptography, security issues and, network and data level security.

Social Science

- New Issues in Security (Politics, POLS 3583)

The course discusses new concepts and challenges for security. Security now embraces military, environmental, economic, social and political sectors. Securitizing problems such as terrorism, gender, human rights, narcotics trade, organized crime, pandemics, and internet abuse has major consequences for state policies, international relations and international organization.

Cape Breton University

Computer Science

- Systems Security and Control (Information Technology, ITEC 3504)

This course provides a systematic approach to computer and information security. It covers methods for auditing computer systems, cost and effectiveness of systems control measures, and fundamentals of implementing a system security program. The development of a Threat and Risk Assessment (TRA) and the review of control objectives for systems are key aspects.

Social Science

- Current Issues in IT - Case Analysis (Information Technology, ITEC 4509)

This course examines the social, legal and ethical issues involved with the use of computer technologies. Topics covered include privacy of information, wiretapping, data encryption, computer crime, intellectual property and professional ethics. This course emphasizes class discussions, case studies, guest lectures and student research presentations.

Dalhousie University

Computer Science

- Usable Privacy and Security (Computer Science, CSCI 6307)

Human factors play an important role in the effectiveness of security and privacy solutions. This course introduces students to several usability and user interface problems related to privacy and security, and to give them experience in designing studies aimed at helping to evaluate usability issues in security and privacy systems.

- Network Security (Computer Science, CSCI 4174)

Security stands out as a critical issue in the design and deployment of information systems in general, and networks in particular. This course will deal with the design of secure information systems with emphasis on secure networking and secure information transfer. It will also include topical and emerging areas in security such as the establishment of an organization-wide security plan and bio-metric identification systems.

- Network Security (Internetworking, INWK 6119)

The primary objective of this course is to provide a comprehensive coverage of the theory, concepts, design principles and technologies for network security. The course focuses on the design principles and techniques of two major aspects of network security: (a) how to secure a network; and (b) how to secure data transactions.

- Introduction to Information Security (Informatics, INFX 2601)

Information security is becoming increasingly important in today's networked world, and is irnpacting every aspect of our lives including finance, healthcare, government, education, SS and entertainment. The objective of this course is to teach the basic principles of information security from the perspective of providing security awareness and its best practices for the real world. Topics include motivation for security, tools and techniques used by adversaries to gather information and launch attacks, Internet security, firewalls, basics of encryption and authentication, virus protection, secure credit card and bank ransactions, wireless security, computer forensics, identity theft and protection, anti-phishing and biometric security.

- Usable Security (Computer Science, CSCI 4169)

Human factors play an important role in the effectiveness of security and privacy solutions, and it is important for security and privacy experts to have an understanding of how people will interact with the systems they develop. This course is designed to introduce students to a

variety of usability and user interface problems related to privacy and security, and to give them experience in designing studies aimed at helping to evaluate usability issues in security and privacy systems. Topics include human threat identification, security warning design, location privacy, privacy policies, web browser privacy and security, phishing, passwords, and secure communication.

- Cryptography (Computer Science/Mathematics, CSCI 4116 and MATH 4116)

This course is an introduction to modern cryptographic techniques and its mathematical foundations. The material covered includes: elementary number theory and algebra, classical cryptosystems, probability, the Data Encryption Standard, prime number generation and primality tests, public key cryptosystems, and further applications, such as digital signatures and identification.

- Advanced Topics in Network Security (Computer Science, CSCI 6708)

This course will provide a comprehensive coverage of the design of secure information systems with emphasis on secure networking and secure information transfer. It will also include topical and emerging areas in security such as wireless network security, mobile device security, security and privacy issues in mobile cloud computing, the establishment of an organization-wide security plan and bio-metric identification systems.

Law and Administration

- Freedom of Information and Privacy Foundations (College of Continuing Education, Local Government Program, -)

Freedom of Information and Privacy Foundations will provide an introduction to the history, theories, and key concepts relevant for the appropriate administration of access and privacy legislation. The course examines access and privacy concepts and principles through the examination of provincial Freedom of Information and Protection of Privacy Acts.

Mount St Vincent University

- Introduction to Information Security (Information Technology, INTE 2285)

A survey of information security and privacy fundamentals. Topics may include threats and defences, legal and ethical issues, risk management, security technologies and business continuity.

- Topics in Information Security (Information Technology, INTE 3385)

An in-depth study of select information security topics. To keep abreast of emerging themes, topics and methods of instruction will vary from year to year.

St Francis Xavier University

- Computer and Network Security (Computer Science, CSCI 467)

Covers the theory and practice of computer and network security, including cryptography, authentication, network security, and computer system security. Topics include secret and public key cryptography; message digests; authentication, including password-based, address-based, and cryptographic; network security; system security, including intruders, malicious software, and firewalls. Students will use and implement algorithms.

St Mary's University

- Communication Networks and Security (Computing and Information Systems, CISY 4436)

This course is an introduction to data communications and computer network systems from a business application perspective. Topics covered include fundamental concepts of data communications, types of communication links, wireless networks, TCP/IP networks, telecommunication and wide area networks. Security topics such as identifying networked enterprise threats, and security technologies for networks for the purposes of secure data transmission and access control, including encryption, authentication, and non-repudiation technologies, are also covered.

- Cryptography (Computing Science, CSCI 4423)

This course provides an introduction to various aspects of data security. Possible topics: classical encryption methods such as Vignere and Vernan ciphers; the Data Encryption Standard; key distribution methods and public key encryption; and authentication using digital signatures. Applications of these methods in the design of protocols for data privacy and security will also be studied.

Ontario

Algoma University

- Information Technology Security and Privacy (Computer Science, COSC 3796)

Computer Security and Privacy is a critical topic in today's world. It is imperative to have an understanding of cryptography, network security, access levels, software development security, as well as security governance and isk management. This course will go over many areas of security and also discuss privacy and its importance. Students will spend time coding, researching, and analyzing algorithms to obtain a greater understanding of security and privacy.

Brock University

Computer Science

- Cryptography and Number Theory (Mathematics and Statistics, MATH 5P92)

Topics may include RSA cryptosystems, ElGamal cryptosystem, algorithms for discrete logarithmic problem, elliptic curves, computing point multiples on elliptic curves, primality testing and factoring algorithms.

- Topics in Number Theory and Cryptography (Mathematics and Statistics, MATH 4P92)

Topics may include algebraic number theory, analytic number theory and cryptography.

Social Science

- Crime, Surveillance and Security (Sociology, SOCI 3P61)

Critical exploration of contemporary efforts to prevent crime, produce order and enhance security through decentralized and proactive initiatives. Conceptions of risk, order and disorder, community and security through examination of topics that may include gated communities, crime stoppers, community policing, urban planning and design, private policing, regulation of public space and surveillance technologies.

Carleton University

- Secure Mobile Networking (Network Technology, NET 4010)

The concept, principle and rationale of mobile networking. Mobile network architecture, protocols, mobility management, routing and mobile TCP/IP; Security challenges, vulnerabilities and threats in mobile networks; Security defense techniques and countermeasures in mobile networks.

- Quantum Computing (Mathematics and Statistics, MATH 5821)

Space of quantum bits; entanglement. Observables in quantum mechanics. Density matrix and Schmidt decomposition. Quantum cryptography. Classical and quantum logic gates. Quantum Fourier transform. Shor's quantum algorithm for factorization of integers.

- Mathematical Cryptography (Mathematics and Statistics, MATH 5300)

Analysis of cryptographic methods used in authentication and data protection, with particular attention to the underlying mathematics, e.g. Algebraic Geometry, Number Theory, and Finite Fields. Advanced topics on Public-Key Cryptography: RSA and integer factorization, Diffie-Hellman, discrete logarithms, elliptic curves. Topics in current research.

- Computer Systems Security (Computer Science, COMP 4108)

Introduction to information security in computer and communications systems, including network, operating systems, web and software security; Passwords, authentication applications, privacy, data integrity, anonymity, secure email, IP security, security infrastructures, firewalls, viruses, intrusion detection, network attacks.

- Computer Security and Usability (Computer Science, COMP 5110)

This course focuses on designing and evaluating security and privacy software with particular attention to human factors and how interaction design impacts security. Topics include current approaches to usable security, methodologies for empirical analysis, and design principles for usable security and privacy.

- Mathematical Cryptography (Mathematics and Statistics, MATH 4809)

Topics covered include: a general survey of public key cryptography; classical applications of finite fields and number theory; relevant background in geometry and algebraic curves; computational issues concerning elliptic curves; elliptic curve cryptosystems; security issues.

- Introduction to Number Theory and Cryptography (Mathematics and Statistics, MATH 3809)

Congruences, distribution of primes, general cryptographic systems, public key cryptographic systems and authentification using number theory, primality testing and factoring in relation to cryptography, continued fractions and Diophantine equations.

- Network Security (Network Technology, NET 3007)

Basics of Information Technology security. Students are introduced to the goals of IT security, common threats and countermeasures including firewalls, SSL technologies and IP Masquerading. Several operating environments will be studied as examples. This course will also include a section on computer ethics.

- Authentification and Software Security (Computer Science, COMP 5407)

Specialized topics in security including advanced authentication techniques, user interface aspects, electronic and digital signatures, security infrastructures and protocols, software vulnerabilities affecting security, untrusted software and hosts, protecting software and digital content.

- Network Security and Cryptography (Computer Science, COMP 5406)

Advanced methodologies selected from symmetric and public key cryptography, network security protocols and infrastructure, identification, secret-sharing, anonymity, intrusion detection, firewalls, defending network attacks and performance in communication networks.

- Designing Secure Networking and Computer Systems (Systems and Computer Engineering, SYSC 5500)

Network security with coverage of computer security in support of networking concepts. Covers various security issues in data networks at different protocol layers. Routing security, worm attacks, and botnets. Security of new mobile networks and emerging networked paradigms such as social networks and cloud computing.

- Wireless Networks and Security (Computer Science, COMP 4203)

An introduction to wireless networks covering both networking issues and security aspects of modern wireless environments. Fundamentals of mobile LANs, ad hoc, sensor networks, secure routing, searching, clustering, multicasting, localization, mobile IP/TCP, confidentiality, key establishment, authentication, broadcasting, RFIDs, and rogue attacks.

- Applied Cryptography (Computer Science, COMP 4109)

Practical aspects of cryptography. Pseudo random number generation, symmetric cryptography (stream and block ciphers), modes of operation, hash functions, message and entity authentication protocols, zero knowledge, pitfalls deploying public-key encryption and digital signatures, key distribution, secret-sharing.

Lakehead University

Computer Science

- Software Safety and Security (Engineering, ENGI 4250)

Network Security: concepts and principles, network security tools (e.g. firewalls, HIDS); Host-Based Safety: fault handling, model checking, static analysis of software, runtime monitoring; Advanced Topics of Security: type-based security, cryptography, authentication, trusted programming, automated theorem proving, proof-carrying code; Ethics and Privacy: security/privacy trade-off, cybercrime, economic and psychological aspects of security.

- Theory of Cryptology (Mathematical Sciences, MATH 3375)

A mathematical introduction to the theory of cryptography and cryptoanalysis.

- Computer Security (Computer Science, COMP 5473)

Several important research topics in one or more of the following areas are investigated: cryptography, computer network security, data security and information security.

- Cryptography and Network Security (Computer Science, COMP 4476)

Topics include conventional encryption, public-key cryptology, authentication and digital signatures, key distribution, IP security, web security, and network management security.

- Cybercrime (Criminology, CRIM 3370)

An introduction to the many different types of cybercrime and the strategies used by law enforcement agencies to deal with this type of crime.

Social Science

- Surveillance and Society (Sociology and Anthropology, SOCI 3811)

An examination of the complex ways that technologies and societies interact to produce feelings of security, fear, control, and/or vulnerability.

McMaster University

Computer Science

- Information Privacy and Security (Computing and Software/eHealth, CAS 767 or eHealth 767)

This course covers issues and technologies in Information Privacy, Security, and Accountability. The course surveys cryptography, digital signature, key management, authentication, certificates, PKI, Application layer Access control policies and mechanisms, data forensics, Internet security protocols, trust management, information and web privacy, privacy and data aggregation, audit log mechanisms, privacy policy expression and enforcement, Differential Privacy, Security and privacy in healthcare, Social networking security and privacy, Usable security and privacy, and privacy-enhancing technologies. Students will undertake a project that employs and integrates these technologies.

- Cryptography (Computing and Software, CAS 762)

An introduction to cryptography: the course will cover public key cryptography based on the discrete logarithm problem, factoring, ellipitic curves and lattices. Thus, it will examine the Diffie-Hellman and El Gamalpkc, RSA as well as lattice-based cryptographic schemes. Other topics will be key-exchange and authentication, identification, schemes, commitment schemes, electronic elections and digital cash, as well as provably secure encryption.

- Cryptography (Mathematical Sciences, MATH 3CY3)

Introduction to cryptosystems used in modern security systems: elementary number theory, primality testing and factorization, discrete logarithm, SRA cryptosystems, elliptic curve cryptosystems.

- Computer Networks and Security (Computer Science/Software Engineering, COMPSCI 4C03/SFWRENG 4CO3)

Physical networks, TCP/IP protocols, switching methods, network layering and components, network services. Information security, computer and network security threats, defence mechanisms, encryption.

- Software Requirements and Security Considerations (Computer Science/Software Engineering, COMPSCI 3RA3/SFWRENG 3RA3)

Software requirements gathering. Critical systems requirements gathering. Security requirements. Traceability of requirements. Verification, validation, and documentation techniques. Software requirements quality attributes. Security policies. Measures for data confidentiality. Design principles that enhance security. Access control mechanisms.

- Information Security (Computer Science, COMPSCI 3IS3)

Basic principles of information security; threats and defences; cryptography; introduction to network security and security management.

- Computer Networks and Security (Computer Science, COMPSCI 3C03)

Physical networks, TCP/IP protocols, switching methods, network layering and components, network services. Information security, computer and network security threats, defense mechanisms, encryption.

- Computer Security (Software Engineering Technology, SFWRTECH 3CS3)

Network and software security, cryptography algorithms, firewalls, vulnerabilities, policies and best practices, attack and defense strategies.

Social Science

- Surveillance and Digital Society (Cultural Studies and Critical Theory, CULTRST 723)

This course explores the issue of surveillance through both theoretical writings and media art practices.

Law and Administration

- Security, Privacy and Trust in eBusiness (Business Administration, BUSINESS K792)

This course discusses important security, privacy, and trust issues and addresses them from business, technology, and government regulation perspectives. Students are required to make seminar presentations and write a research paper on selected topics.

- Privacy, Confidentiality and Security (Health Informatics, Health Information Management, HTH 104)

This course will examine the "concepts, principles and applications of the rights and obligations related to individual access, privacy and confidentiality of personal health information" (CHIMA, 2010, 21). This examination will involve health information data and records in both paper and electronic formats. The course will review legal regulations and legislations currently in place for the collection, use, storing and sharing of personal health information. Learners will study privacy requirements, responsibilities and risks associated with the life cycle of personal health information as Health Information Managers, Health Informaticians, and members of a health care organization. Various legal, ethical and professional standards as they relate to privacy and access will be presented, discussed and critically analyzed from the perspective of the consumer, organization and Health Information professional.

Nipissing University

- Security and Protection (Computer Science, COSC 4607)

This course introduces physical security, privacy, capabilities and access lists, authentication mechanisms and formalisms. The course topics include: overview of system security, security methods and devices, memory protection, recovery management, secure operating systems, hardware/software redundancy.

- Cryptography and Coding Theory (Mathematics, MATH 5247)

Comprehensive discussion of the mathematical foundations of cryptography and cryptanalysis, and the most widely used modern cryptosystems and algorithms. Topics included public key encryption, digital signatures, RSA, Diffie-Hellmann, El Gamal and elliptical curve based cryptography, cryptaalytic attached against them, Shor's Algorithm, quantum cryptography and others as chosen by the instructor.

Queen’s University

Computer Science

- Software Reliability and Security (Computing, CISC 848)

Software crisis and software process models, Software reliability and methods for reliable software, Software reliability engineering process, Software dependability, Software fault tolerance, Run-time software monitoring, Software security, Software security engineering process, Network security, Intrusion detection. Three term hours: lectures and seminars.

- Number Theory and Cryptography (Mathematics and Statistics, MATH 818 and MATH 418)

Time estimates for arithmetic and elementary number theory algorithms (division algorithm, Euclidean algorithm, congruences), modular arithmetic, finite fields, quadratic residues. Design of simple cryptographic systems; public key, RSA systems. Primality and factoring: pseudoprimes, Pollard's rho-method, index calculus. Elliptic curve cryptography.

Social Science

- Advanced Topics in Surveillance Studies (Sociology, SOCY 476)

Advanced study of surveillance engaging with sociological, political, cultural and geographic perspectives. The focus is on core topics in Surveillance Studies including: the relationship between surveillance, power and social control; the concept of privacy, its history, utility and future; surveillance, pleasure and consumption; and surveillance in popular culture.

- Technology and Social Control (Sociology, SOCY 930)

The debate over how technology is implicated in social control is perennial and broad. Relevant twentieth-century theorists include Max Weber, Lewis Mumford, Jacques Ellul, Michel Foucault, Evelyn Fox-Keller, Harold Adams Innis. This course explores the insight and compares the perspectives of selected theorists, and applies them specifically to information and communication technologies. The issue of mass surveillance of populations in the advanced societies, by both government and commercial agencies, is analyzed, both to understand the nature of the social processes involved, and to generate discussion of political and policy implications. While the course is necessarily comparative - globalization is both consequence and cause of technological diffusion - opportunity is given to focus on Canadian examples.

Law and Administration

- IS Security, Privacy and Ethics (Business, COMM 496)

This course examines corporate social responsibility in the information age. Today's managers are responsible not only for the completeness and usefulness of corporate databases but also for securing the personally identifiable information that is stored in their systems and used for decision-making. Companies are responsible to their customers, employees, business partners and governments for ensuring the effective collection, storage, distribution and destruction of this information as well as for its accuracy and appropriate use. Laws such as Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and the U.S, Sarbanes-Oxley Act (SOX) guide corporate actions but managers still must decide how to implement these statutes. This course covers technical issues (e.g., data security controls), behavioural factors e.g., employee and customer actions that expose stakeholders to data losses), legal requirements (such as PIPEDA and SOX) and managerial responsibilities. Cases and guest speakers are utilized to illustrate and underscore the importance of the issues studied.

Redeemer University College

- Computer Assurance Services and Control (Business, BUS 421)

An examination of the control and security of computerized accounting information systems with an assurance services perspective. Topics include professional standards and guidelines for auditing information systems; information technology risks and controls; information systems deployment and management risks; network, telecommunications, and E-Business risks; service organization audits; computer-assisted audit tools and techniques; and conducting the IT audit.

Royal Military College of Canada

- Advanced Network Traffic Analysis (Engineering, EE 593)

There are many benefits to the networking of computer systems, but networks are inherently vulnerable. All networked computing devices are subject to malicious traffic; military networks can be especially attractive targets for espionage services, organized crime and hacking groups. In this course, students will develop a thorough understanding of traffic analysis theory and techniques, and apply these to topical computer security problems such as intrusion detection, extrusion analysis and traffic classification. Specific techniques explored may include intrusion detection systems, signature-based detection and analysis, anomaly-based detection and analysis and traffic classification. Students completing this course will be able to analyse network traffic for the purpose of protecting networks against malicious activity. The course will include practical laboratory work, review and critique of traffic analysis literature and a major course project.

- Cyber Threat and Attack Techniques (Electrical and Computer Engineering, EE 595)

Those operating in the cyber domain who are tasked with the defence of networks and computer systems must have a sound understanding of the threats that they face and of the techniques used by their adversaries; this course discusses the fundamentals of Cyber threats and attack techniques, with a heavy focus on practical applications. Topics will include current cyber threat categories and general capabilities; attack techniques including password cracking, buffer and heap overflows, IP and DNS spoofing, viruses and worms, backdoors and remote access tools, key loggers, tunnelling and covert channels, SQL injection and cross-site scripting; advanced evasion techniques such as polymorphic code and rootkits. The course also introduces malware construction including assembly level program flow control and return oriented programing.

- Introduction to Cryptography (Mathematics and Computer Science, MAE 234)

This course will be an introduction to cryptography including its military, political and mathematical aspects. The course will survey both historical cryptography (antiquity to 1967) and modern (post 1967) cryptography. Students succeeding in this course will understand the workings of important modern techniques including public key cryptography, key exchange protocols and elliptic curve cryptography; both modern encryption and cryptoanalysis will be covered.. More specifically, the following topics will be covered: Historical techniques such as: Alphabetic Ciphers, Frequency Analysis, Vigenere Ciphers, Kaisiski's Method, One Time Pads; The mathematical basis behind modern encryption and decryption: Basic group theory and basic properties of the integers; Modern encryption techniques such as: Public Key Cryptography, RSA, Diffie-Helman Key Exchange, Rabin Encryption, El Gamal, Discrete Log, Elliptic Curves. Modern decryption techniques such as: Birthday Attacks, Quadratic Sieve, Known Plaintext attacks, Man-in-the-middle attacks.

- Computer Systems and Network Security (Engineering, EE 579)

Topics will include computer security concepts, terminology, seminal research, operating systems and issues of network administration related to computer security. Network attack, intrusion techniques and the detection of such attacks and intrusions are explored.

- Secure Communications (Engineering, EE 521)

Direct sequence and frequency hopping spread spectrum systems and their evaluation in the presence of various types of jammer noise. The use of error correcting codes to improve the performance of spread spectrum systems. The study of classical and modern cryptosystems. Public key cryptography and the data encryption standard. Introduction to complexity theory as it pertains to cryptograph.

- Prime numbers and Cryptography (Mathematics and Computer Science, MA 527)

Prime numbers play an important role in many cryptographic methods. This course studies some of the many algorithms linked to prime numbers: deterministic and probabilistic primality tests, generating large primes, factoring methods. Relevant results from theoretical and computational number theory are developed and discussed as needed. Applications of these algorithms in cryptographic methods are also considered.

- Cyber Defence (Engineering, EE 404)

Military and civilian computing systems are frequently attacked by espionage services, organized crime, and hacking groups. In this course, students will investigate the cyber threat environment, network attack, the design of network perimeter defence, and defence-in-depth. The capstone activity is a two-week cyber defence exercise at term end, organized and run by the National Security Agency, involving military college teams from Canada and the United States. Students completing this course will be able to design a defensive computer network architecture and understand the network cyber operations environment. Topics include: firewall design; deployment of intrusion detection and preventions systems; design and implementation of security policy; and identification and authentication.

- Malware Analysis and Forensics (Electrical and Computer Engineering, EE 569)

Dissection of malware for the purposes of understanding, detection and mitigation. Static analysis topics to include hashing, packing and obfuscation techniques, portable executable file format, the execution environment, x86 architecture, code constructs in assembly, the Windows API and registry. Dynamic analysis topics to include sandboxing, run-time debugging, memory maps, threads and stacks, exception handling, drivers and kernel debugging. An introduction to computer forensics to include document-based malware and memory forensic techniques.

- Cryptology (Mathematics and Computer Science, CS 599)

Topics covered include: classical cryptosystems; modern block and stream ciphers; Shannon's information theory; public key ciphers, primality testing, factoring algorithms; digital signatures; unkeyed hash functions and message authentication codes; key distribution and agreement; identification and authentication; pseudo random number generation. Each student will investigate an advanced topic using current research literature.

Ryerson University

Computer Science

- Advanced Topics in Network Security (Engineering, CN 8831)

Students of this course will obtain a firm understanding of the theory and applications of network security. Topics include: AAA mechanisms, secure policy manager, network secure management, Internet security and privacy, and web security. In addition, it covers wireless security fundamentals and addresses common risks and threats on wireless environment.

- Network Security (Computer Engineering, COE 817)

This course provides an introduction to the theory and application of security in computer network environments. Students will develop the skills necessary to formulate and address the security needs of wired and wireless network environments. The course will begin by an overview of network security and cryptography. Latter topics will cover transport level security, IP security, e-mail security, WiFi security, malicious code, firewall, and intrusion detection systems.

- Computer Network Security (Engineering, EE 8213)

This course provides a thorough understanding of technologies and methodologies in network security. It deals with the fundamental techniques used in implementing secure network communications, and forms of attacks on computer networks and approaches to their prevention and detection. Topics that are covered include Introduction to Cryptography, Virtual Private Networks (VPN), Firewalls and intrusion detection techniques. In addition, the course covers worms, viruses, and DDOS attacks and their remedies. Kerberos authentication Protocol, SSL, and anonymous communication protocols.

- Secure Computing (Computer Science, CP 8301)

The importance of security for computer systems: protection, access control, distributed access control, Unix security, applied cryptography, network security, firewalls, secure coding practices, safe languages, mobile code. Computer and network forensics techniques. Computer security techniques. Legal and Ethical issues. Topics may include cryptographic protocols, privacy, anonymity, and/or other topics as time permits.

- Applied Cryptography (Computer Science, CPS 713)

The notion of secure communication. Classical cryptography. Pseudo-random number generation. The Data Encryption Standard and Advanced Encryption Standard. Cryptographically secure hash functions. Public key crypto system. Digital signature schemes. E-commerce and digital cash. Secret sharing schemes. Authentication applications. Electronic mail security. IP and Web security.

- Computer Security (Computer Science, CPS 633)

History and examples of computer crime. Security policies and mechanisms. Access control models. Implementation and usability issues. Physical security. Authentication technologies. Operating system security. Encryption algorithms and protocols. External and internal firewalls. Software flaws and malware. Ethical issues in computer security. Sample privacy noncompliance litigation cases, Social implications of computing networked communication.

- Network Security (Engineering, CN 8816)

This course covers the cryptographic algorithms and secure protocols, and their applications in security mechanisms for computer networks. The course introduces conventional encryption algorithms and Public Key Algorithm with integrity mechanism. Authentication mechanisms for OSI protocols and TCP/IP are also discussed, and their applications in Firewall and IDS (Intrusion Detection System) are studied using actual industrial (for example CISCO's) products.

Social Science

- Security Threats (Criminology, CRM 324)

This course introduces the students to some traditional as well as non-traditional security threats currently challenging Canada and the global community. Students will critically evaluate such topics as transnational organized crime, international terrorism, human trafficking, money laundering and drug trafficking in order to assess the effectiveness of current legal and non-legal methods in dealing with these phenomena.

Law and Administration

- Personal Data Privacy (Management of Technology and Innovation, MT 8321)

The purpose of this course is to identify personal data privacy issues involved in information technology management and examine a full spectrum of possible as well as feasible solutions (technological and business) to safeguard personal data privacy. This course will explore the principles of data privacy, the threats to privacy, international and national policy, particularly privacy enhancing technologies as they apply to the management of information systems and eBusiness.

- Info Sys Security and Control (Management of Technology and Innovation, MT 8324)

This course considers the technical, operational and managerial issues of computer and network security in an operational environment. Industry best practices relating to computer security including schemes for breaking security, and techniques for detecting and preventing security violations are the core focus of this course. Additional material on the development of appropriate safeguards, the study of different types of security systems and the development of appropriate security for the perceived risk are also introduced.

- Auditing of Information Systems (Information Technology Management, ITM 595)

This course is designed to enhance the student's understanding of audit risks and control risks relevant to audits in computerized environments. The course addresses the implementation and evaluation of security and controls in these environments; the techniques necessary to perform external EDP audits; auditing using CAATs; basic considerations in auditing EDI systems; and, audit and control issues associated with eCommerce, networks, VPNs and continuous auditing. The course will focus on auditing of Information Systems, which produce internal and external reports. Students will be introduced to audit approaches, computer risks, concerns related to internal controls and techniques for evaluating systems and business processes. Students will also be able to assess the integrity of data used in various management reports.

- Information Systems Security and Privacy (Information Technology Management, ITM 820)

This course considers the technical, operational, and managerial issues of computer and network security in an operational environment. Industry best-practices relating to computer security including schemes for breaking security, and techniques for detecting and preventing security violations are the core focus of this course. This course will also explore the principles of data privacy, threats to privacy, international and national policy, particularly related to privacy-enhancing technologies as they apply to the management of information systems and e-Business.

Trent University

- Mathematical Cryptography (Mathematics or Computing and Information Systems, MATH 3210 and COIS 3210)

Public vs. private key cryptosystems: cyphertexts, plaintexts, and Kerkhoff's principle. Shannon's theory of perfect secrecy. Modular arithmetic: Chinese reminder theorem, Fermat/Euler theorems. RSA cryptosystem: definition and vulnerabilities. El-Gamal cryptosystem. Rabin cryptosystem. Quadratic residue theory. Probabilistic primality tests and factoring algorithms. Optional: discrete logarithm algorithms and elliptic curve cryptosystems.

- Computer Crime and Forensics (Computing and Information Systems or Forensic Science, COIS 2750 and FRSC 2750)

Computer crime is the fastest-growing area of illegal activity in the world. Users beware! Core topics include the various types of computer crime, including Internet scams, phishing, pharming, identity theft, and sexual predation, as well as the forensic techniques used to follow-up on e-evidence and to prevent victimization.

University of Guelph

Computer Science

- Computer Security (Computer Science, CIS 4110)

This course is a practical survey of the principles and practice of information security.Topics include but are not limited to encryption (symmetric and public key cryptography,key exchange, authentication), security issues and threats (eavesdropping,impersonation,denial of service, viruses, worms, access violations, PKI), system andnetwork security, intrusion detection, access control (DAC, MAC, RBAC), databasesecurity, the common criteria, and threat risk management.

Law and Administration

- Fundamentals of Access, Privacy and Records Information Management (Open Learning and Educational Support, -)

This course will provide participants with an overview of information access and privacy foundations, privacy rights and access to information, and the fundamentals of an effective Records Information Management program. Upon completion, participants will have an understanding of Provincial and other legislation related to privacy, information access and records information management and their relationship in public sector organizations.

- Privacy and Information Management (Open Learning and Educational Support, -)

Access and privacy legislation has impacted the ICT services within today's technology environment. This workshop provides participants with knowledge of legislation and its impact on data access and privacy implications on technology systems. Participants will learn how to facilitate the implementation of privacy and access to information stragtegies to ensure end-user complicance.

University of Ontario Institute of Technology

Computer Science

- Cisco Security I (Business and Information Technology, INFR 2470)

This is part of the Cisco Fundamentals of Network Security that introduces students to design and implement security solutions that will reduce the risk of revenue loss and vulnerability. Topics include: security policy design and management; security technologies, products and solutions; firewall and secure router design, installation, configuration and maintenance; AAA implementation using routers and firewalls; and VPN implementation using routers and firewalls.

- Cisco Security II (Business and Information Technology, INFR 2480)

This is a continuation of the Cisco Security I course, covering security technologies on voice and data communications, wireless LANs, and other related networking technologies.

- Mobile Device Security (Business and Information Technology, INFR 3630)

Mobile devices are becoming part of the everyday life, whether on the individual or enterprise level, and their wide spread is presenting some unique security and privacy challenges to their owners and to any enterprise that allows them to be connected. Some enterprises are even encouraging their employees to bring their own devices (BYOD) in hope of increasing employees connectivity and productivity. The benefits of BOYD can easily be undermined as these mobile devices operates within and outside the security boundaries of an enterprise, are not subject to traditional security compliances, and can easily be stolen and rooted. The objective of this course is to learn about these security challenges and the technologies that can help mitigating them.

- Security (Business and Information Technology, INFR 4420)

This course is the second in the CCIE series to prepare students for the CCIE examination. This course covers expert level knowledge and skill in configuring and maintaining secure networks. CCIE Security certified individuals are experts in the fundamentals of IP and IP routing, as well as the specific area of security protocols and applications.

- OS Security I (Business and Information Technology, INFR 2610)

This course is a definitive security study on Microsoft operating systems, servers, clients, networks, and Internet services. It covers comprehensive security operations and deployment information, along with security tools available on the web.

- OS Security II (Business and Information Technology, INFR 2620)

This course is a definitive security study on Unix operating systems, servers, clients, networks, and Internet services. It covers comprehensive security operations and deployment information, along with security tools available on the web.

- Software and Computer Security (Software Engineering, SOFE 4840)

Introduction to software security, managing software security risk, selecting technologies open vs. closed source, principles of software security, auditing software, buffer overflows, access control, authorization and authentication, race conditions, randomness and determinism, applying cryptography, trust management and input validation, law and ethics of IT security, security at the operating system and network level. Firewalls, intrusion detection.

- Smart Grid Networking and Security (Engineering, ELEE 4125)

Wired and wireless communications in smart grids; communications protocols and standards in smart grid, current and emerging communication technologies; quality and reliability of service in networking for smart grid; security threats and impacts on end-users and utility companies; types of attacks and possible defences; smart grid security, standardization, authentication, and management; user privacy issues.

- Introduction to computer security (Business and Information Technology, INFR 2600)

Introduces the theoretical foundations of IT security. Topics include: fundamental concepts of IT security, vulnerabilities and associated risks, security models, authentication, authorization and accounting (AAA), identity and access control, object protection (granularity, reuse), cryptography, design principles for secure systems, trusted computing base, separation/isolation/ virtualization, malicious logic, logging and auditing, intrusion detection, information security management.

- Emerging IT security technologies (Business and Information Technology, INFR 4620)

This course presents the current trends on research and development in IT security technologies and discusses issues and standards from a technological and management perspective as they relate to the management of large networking systems and computer environments. The course also provides an in-depth examination of IT security hardware and software choices deals with the need to tailor networking operating systems to fit a corporation's enterprise networks.

- Cryptography and Network Security (Business and Information Technology, INFR 3600)

This course covers diverse topics on cryptography and network security. In the cryptography field, students will be exposed to the introductory theory behind symmetric and public-key cryptography, including digital signatures, hash functions, and authentication. The network security section of the course includes topics on authentication, Web security, intruders and firewalls.

- Digital Evidence (Computing Science, CSCI 4120)

This course examines the use of digital information in the examination and analysis of crime scene information and evidence. It covers image and sound analysis and enhancement, pattern recognition techniques, databases, and computer models of criminal activities.

- Forensic Informatics (Computing Science, CSCI 4130)

This is an introductory course in digital forensics, the gathering of evidence from computers that have been involved in a crime. This course covers the use of computers in the commission of crimes, basic evidence gathering techniques, examination of main memory and file systems, network analysis and mobile devices.

- Malware Worms and Viruses (Business and Information Technology, INFR 4630)

This course presents different types of malware, such as viruses, worms, malicious code delivered through web browsers and e-mail clients, backdoors, Trojan horses, user-level Root Kits, and kernel-level manipulation. The course covers characteristics and methods of attack, evolutionary trends, and how to defend against each type of attack.

- Operating System Security (Business and Information Technology, INFR 3610)

This course discusses security solutions for two major Operating Systems: Windows and Unix/Linux. It will cover client/server operation, networking aspects from an OS perspective, as well as Internet services as provided through the OS. It covers comprehensive security operations and deployment information, along with security tools available on the web.

- Cryptography and Secure Communications (Business and Information Technology/Engineering/Information Technology Security, CSCI 5310/ENGR 5670/MITS 5500)

This course covers diverse topics on cryptography and security, including classical encryption, symmetric and public-key cryptography, key management, message authentication, digital signatures, denial-of-service (DoS), distributed DoS, malicious software and intrusion detection systems.

- IT Security (Business and Information Technology, INFR 4610)

This course introduces the concepts and applications of IT security and provides students with the knowledge in exploring the new nature of IT-related threats. The course will provide both technological and social aspects of IT security.

- VPN and Data Privacy (Business and Information Technology, INFR 4650)

This course introduces the development, implementation, and maintenance of Virtual Private Networking (VPNs). Covers topics such as User Authentication and QOS, deployment levels, tunnelling protocols, service level guarantees, and traffic management. Discusses issues on weaving VPN technology into overall information technology infrastructure and study how VPNs facilitate e-commerce, as well as intraorganizational networking.

- Malware and Software Security (Business and Information Technology, INFR 4670)

This course provides a comprehensive study of malicious software (malware), its detection, and its prevention. It explores what vulnerabilities can be exploited by malware (and how), how to identify malware, reverse engineering and debugging, how anti-virus (and other security software) works to detect and remove malware, and how advanced malware tries to evade detection (e.g., obfuscation and encryption). Techniques for preventing and detecting vulnerabilities prior to software release are also covered (e.g., secure programming techniques).

- Secure Software Systems (Business Administration, MITS 5400G)

One of the fundamental causes for most of the computer security problems is insecure software design and implementation. This 243 course takes a proactive approach to cover areas from the technical side of coding secure software to project management tasks. Common coding problems like buffer overflows, random number generation and password authentication are addressed. A secondary focus is placed on a software design process; it needs to be set up so that security is built in at the very early stages, considered throughout the design process and not patched in at a later point of time. From the emerging security technology side, this course also introduces the topics of the eXtensible Markup Language (XML) and a portfolio of related security and privacy standards such as XML Signature, XML Encryption, XML Key Management, WS-Security, SAML, XACML and P3P in response to the growing need for a platform-independent language for supporting interoperable secure software infrastructure. Strategy and policy topics on how to find the right balance between security and usability are addressed as well as the management of a secure software system.

- Malware Analysis (Business and Information Technology, CSCI 5320G)

This course covers diverse topics such as worms, virii, Trojan horses and rootkits ranging from simple JavaScript malicious code to the use of sophisticated malware tools. The course delivers theory with emphasis on practical skills to defend against malware. A sample final project may consist of creating a malware analysis environment to safely capture and study specimens.

- Topics in IT Security (Business and Information Technology, CSCI 5370)

This course covers one or more topics in IT security that are not currently covered by the other courses in the program. The instructor determines the topics that are covered in a particular year and they could change from one year to another. Topics are determined by the instructor before the start of the course. A detailed description of the course content will be posted before the start of term.

- Services Computing Security (Business and Information Technology, CSCI 5710)

This course covers the security-related technologies in services computing. Topics covered include the eXtensible Markup Language (XML) and a portfolio of related security standards such as XML Signature, XML Encryption, XML Key Management, WS-Security and Security Assertion Markup Language (SAML), eXtensible Access Control Markup Language (XACML), the Platform for Privacy Preferences (P3P) and Web X.0, in response to the growing need for a platform independent language for supporting interoperable information in services computing infrastructure. The course provides a services computing context to these more technical issues. Strategy and policy topics on how to find the right balance between security and usability are addressed as well as the maintenance of a secure infrastructure.

- Advanced Topics in IT Security (Business and Information Technology, CSCI 6320)

This course covers one or more advanced topics in IT security that are not currently covered by the other courses in the program. This course is aimed at senior graduate students who have already taken one or more courses in this field. The instructor determines the topics that are covered in a particular year and they could change from one year to another. Topics are determined by the instructor before the start of the course. A detailed description of the course content will be posted before the start of term.

- Operating Systems Security (Business Administration, MITS 5300G)

This course addresses theoretical foundations of IT Security and their implications on the design and operation of operating systems. Operating systems fundamentals are covered to provide a basis for the remainder of the course. The laboratory part of this course puts a particular focus on the Windows and Unix/ Linux operating systems. It provides an overview of the security risk and management of the specified operating systems and preventive efforts to use the security features built within the systems and third-party applications. Students become familiar with essential reference sources available on the subject of computer security, including organizations such as CERT.

- Web Services Security (Business and Information Technology, INFR 4640)

This course presents an overview of web services architecture and issues related to its security. It also introduces ways to build a secure web services system and covers security technologies used for providing secure web services, emphasizing how security works with XML and SOAP.

Social Science

- Cybercrime (Business and Information Technology, BUSI 2570)

This course covers different manifestations of cybercrime including hacking, viruses and other forms of malicious software. It presents technical and social issues of cybercrime, covers the origins and extent of the cybercrime problem, as well as the commercial and political evolution of the computer hacker.

- Trust Systems (Business and Information Technology, INFR 4611)

This course examines the phenomenon of trust across the spectrum from business to information technology. Students will learn about: The impact of trust on business and management, with a principal focus on HR; Trust as a computational phenomenon, its workings and uses, including across reputation systems such as those used in eCommerce; Trust as it applies to cybersecurity. The course is inherently modular and involves exploration of concepts through cases, technical labs, and project work.

- Cybercrime (Criminology and Justice, SSCI 3021)

This course is designed to identify the nature and issues of computer or cybercrime. It will examine the opportunities for cybercrime created by increased reliance on information technology. Specific topics might include cyberterrorism, creation and distribution of viruses, and hacking. It will also examine hacking as both a problem in need of control and a means of controlling cybercrime.

- Cybercrime and Criminology (Criminology, SSCI 5300)

This course explores how a networked world has bred new crimes and new responses and investigates how the computer has become a tool, a target, a place of criminal activity and national security threats, and a mechanism of response. It reviews the origins of these crimes in ordinary crime and traces how these crimes have developed. It examines responses to the emerging threats posed by the various forms of cybercrime and considers the effectiveness of strategies used to combat them. Special topics may include: some in-depth study of predatory stalking, child pornography, hacking, fraud against individuals or companies, and cyber-terrorism. Since these crimes and their prosecution are often transnational, a comparative approach is taken. The course discusses whether national laws are sufficient to regulate international activities and examines international responses to the problem of cybercrime.

Law and Administration

- IT Security Policies and Procedures (Business and Information Technology, INFR 4680)

The objective of this course is to provide an understanding of the need for the multi-disciplinary involvement, an understanding of where this involvement fits into the policy development life cycle and a methodology that provides a means of implementing this development life cycle into an organization. The course discusses how the policy development process should be something that requires the involvement of key business decision makers of which information security is only one.

- Web Services and eBusiness Security (Business and Information Technology, INFR 4660)

This course presents an overview of state-of-the-art e-business security. It examines the most recent attack strategies and offers specific technologies and techniques for combating attempts at data infiltration, destruction, and denial of service attacks. Taking the view that security must be incorporated within multiple levels of e-business technology and practice, the course presents measures for securing system platform, applications, operating environment, processes, and communication links. It shows how the traditional security technologies of firewalls and Virtual Private Networks (VPNs) can be integrated with risk management, vulnerability assessment, intrusion detection, and content management for a comprehensive approach to security.

- IT Forensics (Business and Information Technology, INFR 4690)

In this course, students will learn how to create an incident response plan and implement a computer forensics incident-response strategy, and conduct a proper computer forensics investigation. This course is composed of five pSS: 1) basics, which includes the brief introductions of needed knowledge for this course, such as File System Structures and Metadata, FAT/NTFS/Ext2/Ext3 File System Essentials, Imaging digital media, TCP/IP and networking fundamentals, system administration basics, and information-hiding techniques; 2) computer forensics and investigation, which introduces how to conduct a proper computer forensics and investigation; 3) incident response, which introduces how to create an incident response plan and implement a computer forensics incident response strategy; and 4) case studies, which are completed in teams and one team per case will present their analysis and solution to the class (e.g. in PowerPoint) as it would be done as investigators.

- Information and Privacy Law (Legal Studies, LGLS 2500)

Information and privacy law examines two intersecting yet separate areas of law: privacy law and information law. The privacy law portion of the course will consider the privacy rights protected by the Charter of Rights and Freedoms, public and private sector legislation such as the Privacy Act and the Protection of Personal Information and Electronic Documents Act (PIPEDA), and the development of other causes of action addressing invasion of privacy by individuals. The information law portion will address the principles of open government and open justice, along with analysis of access to information legislation. The interplay between the two areas of law will be a persistent theme throughout the course.

- Auditing Information Systems (Business and Information Technology, BUSI 3172)

This course is designed to introduce and enhance the students' knowledge about the topic of auditing in computerized environments. The course will focus on issues such as information system concepts, audit and control risks, and implementation and evaluation of security and controls.

- Special Topics in IT security (Business Administration, MITS 5610G)

This course focuses on topics in IT Security that are not currently covered by the other courses in the program. Topics may vary depending on the interest of the students and the availability of faculty. A detailed description of the course content will be posted before the start of term.

- Security Policies and Risk Management (Business Administration, MITS 5600G)

This course concerns the role and importance of risk management and security policies. It describes how attackers exploit the interactions between computer systems and their environment in order to learn how to prevent, detect and respond to such attacks. It will also discuss broader business-related security issues such as business continuity, incident recovery and legal issues related to security policies and risk management. Current technologies to aid in implementing security policies and risk management plans will be discussed throughout the course.

- Law and Ethics of IT Security (Business Administration, MITS 5100G)

This course covers the many ways in which commercial law applies to information technology security. As more and more business transactions and communications are now conducted electronically, the IT function within an institution has become the custodian of the official business records. This course introduces the laws governing the daily business of an institution or government agency, as those laws apply to the protection of information and computer systems. Emerging issues, such as privacy and information disclosures, will be discussed in the course.

University of Ottawa

Computer Science

- Computer Security and Usability (Computer Science, CSI 5136)

Design and evaluation of security and privacy software with particular attention to human factors and how interaction design impacts security. Topics include current approaches to usable security, methodologies for empirical analysis, and design principles for usable security and privacy.

- Conception de systèmes informatiques sécuritaires (Computer Engineering/Computer Science, CEG 4799/CSI 4539)

Politiques de sécurité. Mécanismes de sécurité. Sécurité physique. Conscience de la sécurité. Authentification d'utilisateur. Application des mécanismes de sécurité. Codage. "Firewalls" internes et externes. Sécurité des systèmes d'opération et des logiciels. Sécurité des applications de commerce électronique. Conception de systèmes et composantes de sécurité. Dispositifs pour l'analyse de la sécurité, renifleurs, détecteurs d'attaque. Guerre de l'information. Aspects éthiques de la sécurité informatique.

- Internet Security (Electronic Business Technologies, EBC 6170)

User, data and network security principles. Information systems security standards. Security risk analysis frameworks. Fundamentals of Internet security mechanisms including authentication, access control, data encryption and integrity, and Public Key Infrastructure. Internet security including security in the wireless environment. Payment card industry security standards and compliance.

- Designing Secure Networking and Computer Systems (Electrical and Computer Engineering, ELG 6189)

Security issues in data networks and computer systems. The course considers the protocol layers, looks at issues that are associated with specific types of network architectures. Issues with Web security, protocol security and different classes of attacks and defences will also be addressed. Finally, security issues in emerging paradigms, and trends such as social networks and cloud computing, will be addressed.

- Data Encryption (Electrical and Computer Engineering, ELG 5373)

Secure communications: encryption and decryption. Entropy, equivocation and unicity distance. Cryptanalysis and computational complexity. Substitution, transposition and product ciphers. Data Encryption Standard (DES): block and stream cipher modes. Modular arithmetics. Public key cryptosystems: RSA, knapsack. Factorization methods. Elliptic curve cryptography. Authentication methods and cryptographic protocols.

- Authentication and Software Security (Computer Science, CSI 5116)

Specialized topics in security including advanced authentication techniques, user interface aspects, electronic and digital signatures, security infrastructures and protocols, software vulnerabilities affecting security, non-secure software and hosts, protecting software and digital content.

- Network Security and Cryptography (Computer Science, CSI 5105)

Advanced methodologies selected from symmetric and public key cryptography, network security protocols and infrastructure, identification, secret-sharing, anonymity, intrusion detection, firewalls, defending network attacks and performance in communication networks.

- Cryptography (Computer Science, CSI 4108)

The notion of secure communication. Building secure cryptosystems based on the assumption of computational hardness. Cryptographic one-way functions, trap-door functions, pseudorandom generators, and public/private-key encryption schemes. Computational indistinguishable and unpredictability. Digital signature and message authentication. Zero-knowledge/interactive proof systems. Application to e-commerce and e-trade.

- Design of Secure Computer Systems (Computer Engineering/Computer Science, CEG 4399/CSI 4139)

Security policies. Security mechanisms. Physical security. Security awareness. User authentication. Application security mechanisms. Encryption. External and internal firewalls. Security of operating systems and software. Security of e-commerce applications. Design of security system and components. Devices for security analysis; sniffers, attack detectors. Information warfare. Ethical issues in computer security.

- Cryptographie (Computer Science, CSI 4508)

La notion de communication sûre. Construction de cryptosystèmes sûrs fondée sur l'hypothèse de la complexité calculatoire. Fonctions cryptographiques unidirectionnelles, fonctions à portes de déroutement, générateurs pseudo-aléatoires, et schémas de chiffrement à clé publique/privée. Incapacité de distinction et imprévisibilité calculatoires. Signature numérique et authentification de messages. Systèmes de preuves interactifs/à divulgation nulle. Application au commerce électronique et au courtage électronique.

Social Science

- Criminal Justice and Technology (Criminology, CRM 3326)

Theoretical and practical aspects regarding diverse technologies related to criminal justice. Contemporary issues in the matters of surveillance, identification, security and investigation.

- Justice pénale et technologie (Criminology, CRM 3726)

Aspects théoriques et pratiques de diverses technologies en rapport avec la justice pénale. Enjeux contemporains en matière de surveillance, d'identification, de sécurité et d'enquête.

Law and Administration

- Canada and the Cyber Challenge 101 (Security and Policy Institute, Centre for Continuing Education, -)

Computers and information systems are a fundamental part of Canadian life. Day to day activities, commerce, and statecraft have gone digital. The associated information technology underpins nearly all aspects of today's society. It enables much of our commercial and industrial activity, supports our military and national security operations and is essential to everyday social activities. A vast amount of data is constantly in motion and an astronomical quantity is being stored in cyberspace. Furthermore, owing to market incentives, innovation in functionality has outpaced innovation in security and neither the public nor the private sector has been successful at fully implementing existing best practices. The potential for malicious activity within cyberspace is endless. This course will explore the digitized world (the good, the bad and the ugly) in the Canadian context with a view to assessing the breadth and scope of the cyber reality within Canada and the policy challenges it poses with emphasis on the Federal Government. You will be able to identify security gaps that cross policy files, and develop integrated policies to anticipate and respond to cyber threats.

- Privacy Law (Law, CML 3305)

Introduction to Canadian law, policies, practice, and current issues related to the protection of personal information. Focus on the Ontario and federal laws related to privacy, with reference to other provincial and foreign privacy laws, including the Canadian Charter of Rights and Freedoms and the workings of the office of the Privacy Commissioner. Analysis of the policy choices made to mediate the privacy interests of the various stakeholders (the state, the individual, the private sector). Study of both theoretical and practical problems which arise as a result of conflicting views of personal privacy.

- Droit de la communication dans le cyberespace (Law, DRC 4756)

Étude des problèmes juridiques reliés à la réglementation du contenu de l'Internet et à la protection de la vie privée des internautes, envisagés dans divers domaines du droit : communications, diffamation, propos haineux, pornographie, criminalité, protection des renseignements personnels, libertés publiques, etc.

- Regulation of Internet Communication (Law, CML 3395)

Seminar analyzing the legal challenges posed by the Internet to the rights to free speech and privacy. Topics include online obscenity, hate speech, defamation, as well as national and international approaches to data privacy protection.

University of Toronto

Computer Science

- Computer Forensics (Computer Science, CSC 423H5)

Introduction to the digital investigation of electronic evidence. The computer as a crime scene and as a party to a criminal offence. Focus on network issues (intrusion detection, sniffer logs) and operating system issues (especially file system issues: hidden data, file metadata, deleted data). This course will build upon your background in operating systems theory and practice, and will introduce you to the tools and techniques of the computer forensic specialist in the Linux and Microsoft environments. Reference to Canadian computer crime case law.

- Computer Security, Cryptography and Privacy (Electrical and Computer Engineering, ECE 1776H)

The course introduces students to research topics on Computer Security. Students will be introduced to concepts in exploiting vulnerabilities, tools for detection of vulnerabilities, access control models, basic cryptography, and operating system, hardware, and network security.

- Fundamentals of Cryptography (Applied Computing, CSC 2426H)

We will cover the most basic material that is needed for anyone who wants to create or use cryptographic algorithms or protocols. Topics include: Rigorous definitions of security for pseudo-random generators, digital signature schemes, secure hash families, and public-key encryption; methods (including number-theoretic conjectures) for constructing these secure cryptographic primitives; methods for using secure primitives to achieve secure session-key exchange and secure sessions.

- Coding Theory and Cryptography (Computer and Mathematical Sciences, MAT C16H3)

The main problems of coding theory and cryptography are defined. Classic linear and non-linear codes. Error correcting and decoding properties. Cryptanalysis of classical ciphers from substitution to DES and various public key systems [e.g. RSA] and discrete logarithm based systems. Needed mathematical results from number theory, finite fields, and complexity theory are stated.

- Computer and Network Security (Computer and Mathematical Sciences, CSC D27H3)

Public and symmetric key algorithms and their application; key management and certification; authentication protocols; digital signatures and data integrity; secure network and application protocols; application, system and network attacks and defences; intrusion detection and prevention; social engineering attacks; risk assessment and management.

- Computer Security (Electrical and Computer Engineering, ECE 568H1)

As computers permeate our society, the security of such computing systems is becoming of paramount importance. This course covers principles of computer systems security. To build secure systems, one must understand how attackers operate. This course stSS by teaching students how to identify security vulnerabilities and how they can be exploited. Then techniques to create secure systems and defend against such attacks will be discussed. Industry standards for conducting security audits to establish levels of security will be introduced. The course will include an introduction to basic cryptographic techniques as well as hardware used to accelerate cryptographic operations in ATM's and webservers.

- Forensic Computing (Computer Science, CSC 333H5)

Introduction to the tools and techniques of the digital detective. Electronic discovery of digital data, including field investigation methods of the computer crime scene. Focus on the computer science behind computer forensics, network forensics and data forensics. Forensic topics include: computer structure, data acquisition from storage media, file system analysis, network intrusion detection, electronic evidence, Canadian computer crime case law.

- Cryptography and Computational Complexity (Computer Science, CSC 422H5)

A rigorous introduction to the theory of cryptography from the perspective of computational complexity. The relationship of cryptography to the "P=NP" question. As time permits, topics will be chosen from: (i) definitions of different kinds of pseudorandom generators, relationships between them, and ways of constructing them; (ii) secure sessions using shared private key cryptography and public key cryptography; (iii) signature schemes.

- Introduction to Algebraic Cryptography (Computer Science, CSC 322H5)

The course will take students on a journey through the methods of algebra and number theory in cryptography, from Euclid to Zero Knowledge Proofs. Topics include: block ciphers and the Advanced Encryption Standard (AES); algebraic and number-theoretic techniques and algorithms in cryptography, including methods for primality testing and factoring large numbers; encryption and digital signature systems based on RSA, factoring, elliptic curves and integer lattices; and zero-knowledge proofs.

- Computer Security (Computer Science, CSC 427H5)

Network attacks and defenses, operating system vulnerabilities, application security (e-mail, Web, databases), viruses, spyware, social engineering attacks, privacy and digital rights management. The course will cover both attack techniques and defense mechanisms.

- Introduction to Information Security (Computer Science, CSC 347H5)

An investigation of many aspects of modern information security. Major topics cover: Techniques to identify and avoid common software development flaws which leave software vulnerable to crackers. Utilizing modern operating systems security features to deploy software in a protected environment. Common threats to networks and networked computers and tools to deal with them. Cryptography and the role it plays in software development, systems security and network security.

Social Science

- Identity Crime (Sociology, SOC 423H5)

This interactive course concentrates on identity theft and fraud. It provides a critical examination of definitions of, sociological explanations for, and responses to identity crime. Identity crime is examined in the broader context of privacy, national security and organized crime.

- Seminar in Identity, Privacy and Security (Electrical and Computer Engineering, ECE 1518H)

This interdisciplinary course examines issues of identity, privacy and security from a range of technological, policy and scientific perspectives, highlighting the relationships, overlaps, tensions, tradeoffs and synergies between them. Based on a combination of public lectures, in-depth seminar discussions and group project work, it will study contemporary identity, privacy and security systems, practices and controversies, with such focal topics as biometric identification schemes, public key encryption infrastructure, privacy enhancing technologies, identity theft risks and protections, on-line fraud detection and prevention, and computer crime, varying between offerings.

University of Waterloo

Computer Science

- The Mathematics of Public-Key Cryptography (Mathematics, CO 485 and CO 685)

An in-depth study of public-key cryptography. Number-theoretic problems: prime generation, integer factorization, discrete logarithms. Public-key encryption, digital signatures, key establishment, secret sharing. Proofs of security.

- Applied Cryptography (Mathematics, CO 487 and CO 687)

A broad introduction to cryptography, highlighting the major developments of the past twenty years. Symmetric ciphers, hash functions and data integrity, public-key encryption and digital signatures, key establishment, key management. Applications to Internet security, computer security, communications security, and electronic commerce.

- Networking, PC Security and PC Troubleshooting (Professional Development, Centre for Extended Learning, -)

NETWORKING Introduction to Networking Intermediate Networking Wireless Networking PC SECURITY Introduction to PC Security Advanced PC Security PC TROUBLESHOOTING Introduction to PC Troubleshooting.

- Security and Privacy in Health Systems (Computer Science, CS 634)

An overview of basic security and privacy principles relevant in the design and use of applications in health settings. Program security, operating system security, network security, data security, and issues related to the management of security and privacy policies are introduced. Master of Health Informatics students only.

- Computer Network Security (Electrical and Computer Engineering, ECE 628)

Evolution of computer security. Types of security threats, hardware threats, software threats, physical threats, cryptanalysis. The theory of secure message passing. Methods of encryption, private networks, Data Encryption Standard, Public Key Cryptosystems. Secrecy and Privacy in a network environment, long haul networks, local area networks. Protocols for computer network security.

- Computer Security (Electrical and Computer Engineering, ECE 458)

Introduction to computer security. Models of security. Elementary cryptography. Software security, vulnerabilities, threats, defenses and secure-software development processes. Threats to networks and defenses. Security issues at the application layer. Secure design principles, techniques and security evaluation. Privacy, ethics and legal issues.

- Advanced Topics in Cryptography, Security and Privacy (David Cheriton School of Computer Science, CS 858)

No description available.

- Computer Security and Privacy (David Cheriton School of Computer Science, CS 458)

Security and privacy issues in various aspects of computing. Specific topics include: comparing security and privacy, program security, writing secure programs, controls against program threats, operating system security, formal security models, network security, Internet application security and privacy, privacy-enhancing technologies, database security and privacy, inference, data mining, security policies, physical security, economics of security, and legal and ethical issues.

- Quantum Information Processing (David Cheriton School of Computer Science, CS 768)

Review of basics of quantum information and computational complexity; Simple quantum algorithms; Quantum Fourier transform and Shor factoring algorithm: Amplitude amplification, Grover search algorithm and its optimality; Completely positive trace-preserving maps and Kraus representation; Non-locality and communication complexity; Physical realizations of quantum computation: requirements and examples; Quantum error-correction, including CSS codes, and elements of fault-tolerant computation; Quantum cryptography; Security proofs of quantum key distribution protocols; Quantum proof systems. Familiarity with theoretical computer science or quantum mechanics will also be an asset, though most students will not be familiar with both.

- Cryptography / Network Security (David Cheriton School of Computer Science, CS 758)

Cryptographic protocols and their application to secure communication, especially in a network setting. Identification and entity authentication; protocols for key establishment, transport, agreement and maintenance; secret sharing, broadcast encryption, tracing schemes; certificates, public-key infrastructure, PGP.

- Computer Security and Privacy (David Cheriton School of Computer Science, CS 658)

Security and privacy issues in various aspects of computing. Specific topics include: comparing security and privacy, program security, writing secure programs, controls against program threats, operating system security, formal security models, network security, Internet application security and privacy, privacy-enhancing technologies, database security and privacy, inference, data mining, security policies, physical security, economics of security, and legal and ethical issues.

- Cryptography and System Security (Electrical and Computer Engineering, ECE 409)

Introduction to cryptology and computer security, theory of secure communications, points of attack, conventional cryptographic systems, public key cryptographic systems, standards, firewalls, wireless system security, applications.

Social Science

- Surveillance and Society (Sociology and Legal Studies, SOC 413)

An examination of the way monitoring technologies alter and shape social life in terms of security, fear, control, and vulnerability.

University of Windsor

Computer Science

- Data Security and Cryptography (Computer Science, 88-566)

This is an introductory course on the techniques, algorithms, architectures and tools of data security and cryptography. Firstly, the theoretical aspects of data security and cryptographic algorithms and protocols are reviewed. Then we show how these techniques can be integrated to provide solutions to particular data and communication security problems. This course contents are of use to computer and communication engineers who are interested in embedding security services into an information system, and thus, providing integrity, confidentiality and authenticity of the data and the communicating parties.Main contents: classical cryptography techniques; mathematical foundations; secret key cryptography; public key cryptography; authentication and digital signature; network cryptographic protocols.

- Computer Networks Security (Electrical and Computer Engineering, 88-447)

Introduction to computer networks security; cryptography; public-key and secret key encryption; encryption algorithms; network security mechanisms and techniques; security protocols; authentication and network security services; traditional and emerging Information Technology (IT) security; cyber-security.

- Security and Privacy on the Internet (Computer Science, 60-564)

This course introduces the issues of security in public distributed networks. Topics include: security planning, policies and procedures, threats and strategies, security services and mechanisms, digital rights; topics in Internet related to security and privacy; secure protocols, DES, AES; public key algorithms; VPN; Internet sniffing and scanning tools; intrusion detection, intrusion analysis and tools; viruses and enterprise anti-virus tools; other applications such as digital cash, code signing and anonymous e-mail.

- Network Security (Computer Science, 88-558)

The course presents a concise discussion on the discipline of cryptography- covering algorithms and protocols underlying network security applications, encryption, hash functions, digital signatures, and key exchange. Internet security vulnerabilities, firewalls and their limitations, cryptographic technology and services, PPP and data layer security, IPSec and key management for network layer security, TLS, SSH and transport layer security, secure e-mail, secure infrastructure protocols, Kerberos authentication, secure RPC, remote authentication, authorization and tunneling protocols, virtual private networks, secure remote access, multicast security are covered.

- Network Security (Computer Science, 60-467)

This course will introduce students to advanced topics in network security. Topics will include encryption and authentication techniques, detection and analysis of intrusions, and the security of electronic mail and web access.

- Networking and Data Security (Computer Science, 60-667)

This course will introduce students to the fundamental concepts of computer networks, with an emphasis on network security. Topics will cover fundamental principles and protocols of computer networks, types of security threats and vulnerabilities and a variety of techniques for addressing security issues, such as security protocols, firewalls, intrusion detection/prevention.

Social Science

- Privacy, Surveillance and Security in the Digital Age (Communication, Media and Film, 40-304)

This course provides an historical examination of the conceptual apparatuses that have traditionally framed understandings of the right to privacy, critically assesses the capacities of the State and corporate entities to monitor digital activities and explores the social, political and economic implications of surveillance practices. Topics may include: user-generated surveillance, mobile technologies, cloud computing, geo-locating technologies, tracking software, and data mining in social media contexts.

- Surveillance and Society (Sociology, Anthropology and Criminology, 48-382)

The course provides an overview of surveillance in contemporary society. Substantive topics may include surveillance in relation to national security, covert police activities, social media, consumers, workplace, biometrics and inequality, social sorting, privacy, and privacy law/regulation. Focus of the course will vary by instructor.

Western University

Computer Science

- Cryptography and Security (Computer Science, CS 9534)

Principles and practice of cryptography and network security: classical systems, symmetric block ciphers (DES, AES, other contemporary symmetric ciphers), linear and differential cryptanalysis, perfect secrecy, public-key cryptography (RSA, discrete logarithms), algorithms for factoring and discrete logarithms, cryptographic protocols, hash functions, authentication, key management, key exchange, signature schemes, security.

- Introduction to Hacking: Exploitation and Protection of Systems and Software (Electrical and Computer Engineering, ECE 9609 and ECE 9069b)

Sometimes it seems like ever time you read the news there's a story about a new security vulnerability. Have you ever wondered how these vulnerabilities come about, and how they are discovered and exploited? This course will introduce you to basic concepts and techniques used in the exploitation of systems and software (i.e., hacking). From activists to cyber criminals to national security agencies, hackers are an inescapable reality of the information age. The goal of this course is, as the saying goes, to know your enemy so that you might defend yourself against them.

- Physical Layer Security of Information (Electrical and Computer Engineering, ECE 9320 and ECE 9032)

The aim of the first part of the course is to introduce concepts of cybersecurity and protection of information on physical layer. The course provides theoretical foundation of corresponding techniques and developes practical skills in simulation and evaluation of cybersecurity of communication systems on the link level.

- Database Security and Privacy (Computer Science, CS 9616)

This course considers access control as it relates to databases. Different access control models will be discussed, as well as how they apply to different database models: relational, object-oriented and XML databases for example. Statistical database querying issues will be covered. Privacy of data in a database will also be examined.

- Information Systems Audit (Management and Organizational Studies, MOS 4464)

Students will examine audit and control procedures in a computerized environment in order to develop the skills needed to analyze an organization's computer and information systems in order to evaluate the integrity of its production systems as well as potential security concerns.

- Cryptography and Security (Computer Science, CS 9534)

Principles and practice of cryptography and network security: classical systems, symmetric block ciphers (DES, AES, other contemporary symmetric ciphers), linear and differential cryptanalysis, perfect secrecy, public-key cryptography (RSA, discrete logarithms), algorithms for factoring and discrete logarithms, cryptographic protocols, hash functions, authentication, key management, key exchange, signature schemes, security.

- Cryptography and Security (Computer Science, CS 4413)

Survey of the principles and practice of cryptography and network security: classical cryptography, public-key cryptography and cryptographic protocols, network and system security.

- Information Security (Software Engineering, SE 4472)

This course provides an introduction to the topic of security in the context of computer networks. The goals are to provide students with a foundation allowing them to identify, analyze, and solve network-related security problems in information systems with the emphasis on the engineering aspects of information security.

Social Science

- Social Networking in Everyday Life: Social Relations, Social Movements, and Privacy (Media, Information and Technoculture, MIT 3374)

This course will investigate the term social networking and its related theories. We will examine various platforms and the social consequences these have had for our understanding of friendship, work, and privacy. Our aim is to not only have a good understanding of the theories of social networking, but also of the methodological approaches that exist to study how social networking unfolds.

- Privacy and Surveillance (Information and Media Studies, LIS 9134)

This seminar course explores control and freedom in the information age by examining technologies, institutions, representations and practices of surveillance in libraries, archives and databases. It also examines related issues of intellectual freedom, content filtering and copyright management. These topics are investigated through theoretical discussion, case studies, and research presentation.

Wilfrid Laurier University

- Applied Cryptography (Computer Science, CP 460)

Algorithms and issues in applied cryptography. Topics include history of cryptography, block ciphers, stream ciphers, public-key encryption, digital signatures and key management. Also, discussions of current issues in information security.

- Number Theory and Cryptography (Mathematics, MA 617)

This course introduces topics from number theory with application to public key cryptography. Topics include: elementary number theory; quadratic residues; quadratic reciprocity; finite field arithmetic; elliptic curve groups; RSA public-key cryptography; elliptic curve cryptography; the discrete logarithm problem for elliptic curves; and algorithms for primality testing and factoring.

York University

Computer Science

- Mathematics of Cryptography (Electrical Engineering and Computer Science/Mathematics, EECS 4161/MATH 4161)

Probability, information theory and number theory and applications to cryptography. Classical codes such as Caesar shift, Vigenere, ADFGVX, rectangular substitution, and others. Other topics: comma free codes, perfect secrecy, index of coincidence, public key systems, primality testing and factorization algorithms.

- Computer Security Management: Assessment and Forensics (Electrical Engineering and Computer Science, EECS 4482)

This course examines the organizational policy and management aspects of computer security. It covers topics such as policies, procedures, and standards related to access and use, compliance and privacy, risk management and incident response.

- Computer Security Laboratory (Electrical Engineering and Computer Science, EECS 4481)

This course provides a thorough understanding of the technical aspects of computer security. It covers network, operating systems, and application software security. Computer laboratory projects provide exposure to various tools in a hands-on setting.

- Introduction to Computer Security (Electrical Engineering and Computer Science, EECS 3482)

This course introduces fundamental computer security concepts. Topics include security goals and terminology, an overview of the various security domains, an introduction to cryptography, security policies, risk management and auditing. Laboratory exercises emphasize these topics in a practical manner.

- Applied Cryptography (Electrical Engineering and Computer Science, EECS 3481)

An overview of cryptographic algorithms and the main cryptosystems in use today, emphasizing the application of cryptographic algorithms to designing secure protocols.

- Mission-Critical Systems (Electrical Engineering and Computer Science, EECS 4315)

Theory and practical tools underlying deductive and algorithmic methods for ensuring the safety and correctness of mission critical systems (e.g. medical systems, nuclear reactors and train systems) with the practical ability to use verification tools to perform software certification.

- Computer Security Project (Electrical Engineering and Computer Science, EECS 4480)

This is a capstone project course for computer security students. The students engage in a significant research and/or development project that has major computer security considerations.

Social Science

- Crime, Science and Technology (Criminology, CRIM 3658)

This course examines how science and technology have altered the terrain of criminal justice and criminology. It focuses not only on the ways in which criminology has been constructed as a science, but also the ways in which technology has created new crimes, new forms of identity (e.g. data doubles), and new spaces that need to be policed (e.g. cyberspace). Topics include fingerprinting, DNA testing, biometrics, surveillance technologies, the regulation of mobilities, the use of robots, and cybercrime.

Law and Administration

- Privacy and the Law (Law and Society, LASO 3365)

This course examines contemporary legal doctrines of privacy with special attention paid to the underlying socio-political transformations they embody. The course will examine in detail the dilemmas facing privacy law in the age of social media.

Quebec

Bishop's University

- Computer and Networking Security (Computer Science, CS 325)

This course provides an introduction to security and privacy issues in various aspects of computing, including cryptography, software, operating systems, networks, databases, and Internet applications. It examines causes of security and privacy breaches, and gives methods to help prevent them.

- Cryptography (Mathematics, MAT 324)

Cryptography is a key technology in electronic security systems. The aim of this course is to explain the basic techniques of modern cryptography and to provide the necessary mathematical background. Topics may include: the classical encryption schemes, perfect secrecy, DES, prime number generation, public-key encryption, factoring, digital signatures, quantum computing.

Concordia University

Computer Science

- Cybercrime Investigations (Information Systems Engineering, INSE 6610)

Introduction to cybercrimes: unauthorized access, mischief to data, possession of hacking tools, possession of child pornography; Legal aspects: Canadian judicial system, computer crime laws, charter of rights, common law, mutual legal assistance treaty, search warrants, production and assistance orders, international laws, upcoming legal changes; Investigation process: search planning, acquisition methods, environment recognition, evidence identification; Reporting process: investigation and analysis reports, notes taking; authority of seizure; forensic interviews; Computer crime trials: witness preparation, court sentencing, rebuttal witness, cross-examination, testimony, credibility attacks; in-depth case studies. A project.

- Wireless Network Security (Information Systems Engineering, INSE 6190)

Introduction to wireless network security; security issues in cellular networks; authentication/key management in wireless LAN; secure handover; security in mobile IP; security issues in mobile ad-hoc networks: trust establishment, secure routing, anonymity; anonymous sensory data collection; privacy for smartphone applications.

- Cloud Computing Security and Privacy (Information Systems Engineering, INSE 6620)

Cloud computing concepts, SOA and cloud, virtualization and cloud, cloud service delivery models, cloud storage models, cloud deployment scenarios, public/ private/ hybrid/ community cloud, cloud computing architectures, SaaS, PaaS, IaaS, agility, scalability and elasticity of cloud, cloud security, cloud privacy, homomorphic encryption, searching encrypted cloud data, secure data outsourcing, secure computation outsourcing, proof of data possession / retrievability, virtual machine security, trusted computing in clouds, cloud-centric regulatory compliance, business and security risk models, cloud user security, identity management in cloud, SAML, applications of secure cloud computing.

- Recent Developments in Information Systems Security (Information Systems Engineering, INSE 6630)

Security and privacy legislations. New security threats and solution on personal computers, enterprise computers, personal information, confidential information, identity fraud, financial fraud, and social networking. Recent developments in trusted computing for critical cyber infrastructure, privacy-aware information sharing, cybercrime, and cyber forensics techniques. Cyber espionage, cyber terrorism, and cyber war.

- Smart Grids and Control System Security (Information Systems Engineering, INSE 6640)

Overview of electric grid operation, evolution to the smart grid, smart grid components, dynamic pricing, promotion of "green" resources, governmental regulation, network standards, consumer privacy, risks to the smart grid, physical security and protections against tampering for smart grid environments, device level security, authorization and access control, consumer privacy protection, cryptographic mechanisms for smart grid environments, secure key management, communication security in smart grid, privacy of user data for Advanced Metering Infrastructure (AMI), security standards for smart grid, supervisory control and data acquisition (SCADA), SCADA architecture, SCADA Security, SCADA monitoring, SCADA systems for smart grids, distributed control systems (DCS), communication infrastructure.

- Trusted Computing (Information Systems Engineering, INSE 6650)

Hardware and software root of trust; establishing and attesting trust of software systems; Trusted Platform Module (TPM); CPU support for trusted computing, including existing technologies such as Intel Trusted Execution Technology (TXT), AMD Secure Virtual Machine (SVM), ARM TrustZone; secure crypto processors such as Hardware Security Modules (HSMs); bank HSM APIs and their weaknesses; attestation protocols; OS support for trusted computing; security tokens (e.g., second factor of authentication, smartcards, transaction verification code); trusted user interface; use cases: digital rights management (DRM), authentication, protected execution of security sensitive code, trusted kiosk computing, full disk encryption, malware exploiting trusted computing infrastructure; hardware and software attacks; privacy issues.

- Networks Security and Management (Engineering, ELEC 465)

Network security threats. Importance of security policy. Principles and techniques of encryption and authentication. Network security protocols: X509, IPSEC (Internet Protocol Security Architecture). Network management: issues, architectures, and protocols. Fault management, configuration management, security management, performance management, and accounting management. Management Information Bases (MIBs). SNMP and its evolution.

- Database Security and Privacy (Information Systems Engineering, INSE 6160)

Access control in relational databases; grant/revoke model; security by views; query modification; Oracle VPD; auditing in databases; information warfare in databases; multi-level database security; polyinstantiation and covert channel; statistical database security; inference control; security by auditing; microdata security; random perturbation; outsourced database security, encrypted databases; SQL injection attack; anomaly detection in databases; data privacy, P3P; Hippocratic databases; perfect secrecy-based privacy; k-anonymity model; l-diversity; data utility measure, data release with public algorithms, multi-party privacy preserving computation; privacy in OLAP.

- Design and Analysis of Security Protocols (Information Systems Engineering, INSE 7100)

The primary objective of this course is to present the methods used in the design and analysis of modern security protocols, introduction to existing cryptographic protocols. The most important security proprieties (such as authentication, secrecy, integrity, availability, atomicity, certified delivery and other properties), flaw taxonomy (such as freshness attacks, type attacks, parallel session attacks, implementation dependent attacks, binding attacks, encapsulation attacks and other forms of attack). Cryptographic protocol specification (general-purpose formal languages, logical languages, operational languages and security calculi). Cryptographic protocol analysis (security logics analysis, model-based and algebraic analysis, process algebra analysis, type based analysis). Limitations of formal methods and ad-hoc techniques, project will be offered in analyzing a number of published cryptographic protocols. The focus of this course will be on the design and the analysis of security protocols.

- Network Security Architecture and Management (Information Systems Engineering, INSE 6170)

Security architecture and management, risk and threats, security attributes and properties, security design principles, security standards, security defence toolkit, and security building blocks, corporate VoIP, residential IPTV, IMS, cloud services, security functions and their implementation, operational considerations of deployment and management of security, configuration, vulnerability management and updates, incident management, emerging challenges and innovative solutions.

- Security Evaluation Methodologies (Information Systems Engineering, INSE 6150)

Security evaluation of information systems, security evaluation of software, security evaluation of products. Security code inspection, security testing, security standards, preparation of a security evaluation: impact scale, likelihood scale, severity scale. Vulnerability analysis, risk analysis, security plan elaboration. ITSEC, MARION, and MEHARI methods, OCTAVE, common criteria, target of evaluation, protection profile, security functional requirement, security factors, errors, accidents, assurance requirements, assurance levels, evaluation process, compliance with the protection profile, IT security ethics, privacy, digital copyright, licensing IT security products, computer fraud and abuse, incident handling, business records, security forensics, security evaluation case studies. Information security governance: risk management, business strategy, standards, COBIT. Situation awareness.

- Malware Defenses and Application Security (Information Systems Engineering, INSE 6140)

Malicious code, taxonomy, viruses, worms, trojan horses, logical and temporal bombs, infection process, security properties of applications, safety, high level security, detection approaches, ad hoc techniques: scanning, anti-virus technology, obfuscation, dynamic analysis for security: passive and active monitoring, in-line and reference monitors, sandboxing, static analysis for security: data and control flow analysis for security, type-based analysis for security, anti-reverse-engineering protection, software fingerprinting, self-certified code: certifying compilers, proof carrying code, efficient code certification, typed assembly languages, certificate generation, certificate verification and validation, C and C++ security, java security, byte-code verification, access controllers, security managers, permission files, security APIs, critical APIs, protection domains, security profiles, mobile code security.

- Operating Systems Security (Information Systems Engineering, INSE 6130)

System security, Windows security, Linux security, Unix security, access control matrix, HRU result, OS security mechanisms, security administration, access control list, capability list, role-based access control, security policy, mandatory and discretionary access control, multi-level security, BLP policy, Biba model, conflict of interest, Chinese Wall policy, secure booting, authentication, password security, challenge response, auditing and logging, system kernel security, threat analysis, security attacks, security hardened operating, host-based intrusion detection, securing network services, firewalls and border security, registry security, embedded and real-time OS security, information flow control.

- Crypto-Protocol and Network Security (Information Systems Engineering, INSE 6120)

Cryptographic protocols, authentication protocols, key distributions protocols, e-commerce protocols, fair-exchange and contract-signing protocols, security protocol properties: authentication, secrecy, integrity, availability, non-repudiation, atomicity, certified delivery, crypto-protocol attacks, design principles for security protocols, automatic analysis, public key infrastructure, models and architectures for network security, authentication using Kerberos and X.509, email security (PGP, S/MIME), IP security, SSL/TLS protocols, virtual private networks, firewalls intrusion detection, host-based IDS, network based IDS, misuse detection methods, anomaly detection methods, intrusion detection in distributed systems, intrusion detection in wireless ad hoc networks botnet detection, analysis and mitigation, darknet traffic analysis, prediction and forecast of network threats, network security monitoring.

- Fundamentals of Modern Cryptography (Information Systems Engineering, INSE 6110)

Introduction to cryptography and cryptanalysis, classical ciphers, number-theoretic reference problems, the integer factorization problem, the RSA problem, the quadratic residuosity problem, computing square roots in Zn, the discrete logarithmic problem, the diffie-hellman problem, pseudorandom bits and sequences, stream ciphers: feedback shift registers, LFSRs, RC4. Block Ciphers: SPN and Fiestel structures, DES, AES, linear cryptanalysis, differential cryptanalysis, side channel attacks, ciphertext indistinguishability, attack analysis, IND-CPA, IND-CCA, IND-CCA2, public key encryption: RSA, Rabin, ElGamal, elliptic curves cryptography, hash functions: Un-keyed hash functions, MACs, Attacks, Digital signatures: RSA, Fiat-Shamir, DSA, public key infrastructure, key management, efficient implementation of ciphers, zero-knowledge proof.

- Cryptography and Data Security (Computer Science and Software Engineering, COMP 7521)

Traditional cryptography. Information theory. Private-key (symmetric-key) and public-key (asymmetric-key) cryptographic algorithms. Advanced Encryption Standard (Rijndael). Cryptographic hash functions. Digital signatures. Data-origin authentication and data integrity. Entity authentication. Key distribution, management, recovery, and exhaustion. Authentication protocols. Security services (confidentiality, authentication, integrity, access control, non-repudiation, and availability) and mechanisms (encryption, data-integrity mechanisms, digital signatures, keyed hashes, access-control mechanisms, challenge-response authentication, traffic padding, and routing control).

- Information Systems Security (Computer Science and Software Engineering, SOEN 321)

Protocol layers and security protocols. Intranets and extranets. Mobile computing. Electronic commerce. Security architectures in open-network environments. Cryptographic security protocols. Threats, attacks, and vulnerabilities. Security services: confidentiality; authentication; integrity; access control; non-repudiation; and availability. Security mechanisms: encryption; data-integrity mechanisms; digital signatures; keyed hashes; access-control mechanisms; challenge-response authentication; traffic padding; routing control; and notarization. Key-management principles. Distributed and embedded firewalls. Security zones.

- Security and Privacy Implications of Data Mining (Information Systems Engineering, INSE 6180)

Introduction to data mining and its applications; privacy legislations security and privacy threats caused by current data mining techniques; risks and challenges in emerging data mining applications; attacks and prevention methods: web privacy attacks, data mining-based intrusion detection; privacy-preserving data mining; privacy-preserving data publishing.

Law and Administration

- Auditing Information Systems (Information Systems and Audit Control, Centre for Continuing Education, CEIS 959)

This 40-hour course develops the knowledge necessary to provide audit services, in accordance with IT audit ISACA standards, to assist the enterprise with protecting and controlling information systems.

- Protection of Information Assets (Information Systems and Audit Control, Centre for Continuing Education, CEIS 920)

This 50-hour course focuses on key points of the protection of IS assets. It includes security standards as drafted in policies, controls over the confidentiality, integrity and availability of IS, data classification practices, as well as the physical controls and processes following the life cycle of information assets. The course covers best practices in the information security management industry, from incident management to backups and restoration procedures.

École de technologie supérieure

Computer Science

- Tests de vulnérabilité : organisation et communication des résultats (Perfectionnement et formation continue, -)

Objectifs : Distinguer les différents types de tests de sécurité. Déterminer les étapes à suivre pour différents types d'analyses de sécurité. Évaluer le temps requis pour une activité d'analyse de sécurité. Ajuster un calendrier pour prévoir la réalisation des analyses de sécurité appropriées dans les temps accordés à un projet. Rédiger un rapport décrivant les tests de sécurité et l'analyse des résultats obtenus. Déterminer, documenter et assurer le suivi d'un plan d'action des suites d'une analyse de sécurité basé sur la gestion des risques. Présenter efficacement les résultats d'une analyse de sécurité.

- Mobilité et infonuagique : enjeux pour la sécurité de l’information (Perfectionnement et formation continue, -)

Dans un contexte de mobilité et de renouveau des dynamiques de travail (télétravail, recours à des fournisseurs de services logiciels en ligne, etc.), cette formation est offerte aux gestionnaires et aux spécialistes de la sécurité de l'information afin de les sensibiliser aux enjeux de sécurité créés par ces nouvelles technologies.

- Sécurité des infrastructures TI : les meilleures pratiques (Perfectionnement et formation continue, -)

Objectifs - Identifier les composantes qui jouent un rôle clé dans la sécurité des systèmes d'exploitation. - Identifier les outils nécessaires à la sécurisation d'un système informatique en fonction des besoins. - Appliquer les meilleures pratiques en regard à la sécurité dans l'exécution des tâches d'administration de systèmes. - Définir et mettre en oeuvre une politique de contrôle d'accès. - Renforcer la protection d'un système en réduisant la surface d'attaque (bastionnage). - Installer et configurer des outils de surveillance et de protection au niveau du système d'exploitation. - Configurer et gérer les mécanismes de journalisation.

- Sécurité des réseaux d'entreprise (Génie logiciel et des technologies de l'information, GTI 719)

Ce cours a pour principal objectif de présenter les aspects essentiels de la sécurité des systèmes d'information des entreprises : méthode d'analyse de risque, sécurité des principales composantes des infrastructures TI, gestion des incidents, plans de relève, audits, politiques de sécurité et gouvernance.

- Sécurité de l'internet (Génie logiciel et des technologies de l'information, MGR 850)

Problématique de la sécurité. Terminologie. Notion de confiance. Identification des faiblesses d'Internet. Types d'attaques possibles contre chacune des faiblesses. Analyse des risques. Enjeux d'éthique. Mécanismes de protection disponibles. Pratiques préventives. Contre-mesures. Techniques de cryptographie. Mécanismes de base.

- Sécurité des systèmes (Génie logiciel et des technologies de l'information, GTI 619)

Ce cours aura pour principal objectif de présenter les principaux aspects de la sécurité des systèmes reliés aux technologies de l'information: analyse de risque, vulnérabilités applicatives et protocolaires, menaces informatiques, contre-mesures classiques. De plus, les impacts de la sécurité sur le cycle de développement logiciel seront aussi présentés.

- Sécurité des systèmes informatiques (Génie, INF 8750)

Principes et concepts fondamentaux de la sécurité des systèmes informatiques. Principaux services: confidentialité, intégrité, disponibilité, authentification, non répudiation, contrôle d'accès. Typologie des attaques: fuites, modifications d'information, privations de service. Mécanismes sécuritaires modernes: systèmes de chiffrage symétriques et asymétriques; fonctions de hachage; génération pseudo-aléatoire. Protocoles sécuritaires: authentification, signature, échange et gestion de clés. Sécurité des systèmes centralisés et des systèmes répartis: politiques et modèles de sécurité; contrôle d'accès; rôles et privilèges. Sécurité des programmes: virus, chevaux de Troie. Contre-mesures: journalisation, audits; détection d'intrusion; filtrage; mécanismes de recouvrement. Analyse de risque. Éducation des usagers. Considérations légales, politiques et éthiques.

Law and Administration

- ISO 27001 : mise en place d'un système de management de la sécurité de l'information (Perfectionnement et formation continue, -)

La norme ISO/CEI 27001 est une norme liée à la gestion de la sécurité de l'information. Elle décrit, sous forme d'exigences, les pratiques (organisation, techniques, etc.) à mettre en place pour qu'une organisation puisse maîtriser efficacement le risque lié à l'information. Cette formation permet de comprendre l'implication d'un système de gestion de la sécurité de l'information (SMSI) dans le contexte d'ISO 27001.

École Polytechnique de Montréal

Computer Science

- Aspects électroniques de l'informatique judiciaire (Centre de formation continue, CF 150)

Intervention physique sur le média ou l'ordinateur examiné. Composants de base d'un ordinateur. Extraction de disque dur. Installation et paramétrage de systèmes d'exploitation courants. Connaissance générale des systèmes d'exploitation de serveur. Outillage d'informatique judiciaire, bloqueurs et câblages. Ateliers de pratique manuelle. Image, copie et clone des médias à l'aide de logiciels ou de machines. Mode général d'écriture d'un média (disque dur, disquette, ruban, CD). Systèmes de fichiers courants excluant NTFS. Examen d'agenda électronique et de cellulaire.

- Outils de sécurité réseau (Centre de formation continue, CR 150)

Défense passive d'un réseau. Logiciels et équipements de surveillance et de contrôle de l'activité d'un réseau : installation et configuration, synchronisation de mesures. Détection des intrusions et des maliciels Mesures à exclure et mesures incompatibles. Détection et prévention des utilisations illégitimes de réseau. Réseau domestique : protection à peu de frais. Configuration d'un routeur à large bande et de modem Internet.

- Sécurité et architecture des réseaux informatiques (Centre de formation continue, CR 160)

Composantes de réseaux informatiques et architecture réseau dans un contexte de sécurité : postes de travail, serveurs, applications Web, bases de données, routeurs, commutateurs, point d'accès sans fil, voix sur IP (VoIP), pare-feu, systèmes de détection d'intrusion (IDS), serveur mandataire (Proxy), antivirus, courriels, filtrage de contenu (filtrage URL), corrélateurs d'évènements (SIMS/SEMS), authentification, serveurs de journaux, surveillance réseau. Virtualisation. Standards, normes et lois. Principes d'architecture réseau et de sécurité : zones, flots de trafic, sécurité interzone, Intranet, Extranet, Internet, LAN / WAN, VPN. Relations entre les diverses composantes de réseau et de sécurité. Analyses de vulnérabilité. Honeypot.

- Concepts avancés en sécurité informatique (Génie, INF 6422)

Évaluation de performance en sécurité informatique. Performance des systèmes défensifs vs performance des outils d'attaques. Méthodes quantitatives d'évaluation de performance en sécurité informatique : modèles mathématiques, simulation et émulation. Méthodes d'expérimentation en laboratoire. Systèmes de détection d'intrusion (IDS) : recherche, déploiement commercial et limitations. Détection par règle et par anomalie. Évasion d'IDS et attaques par imitation. Détection de code malicieux : principes de base et problématiques actuelles. Réseaux de zombies : types, historique et fonctionnement. Méthode de détection et de mitigation. Attaques de déni de service : utilisation à des fins économiques et politiques, solutions proposées et utilisées. Modèles sémantiques des concepts de sécurité et attaques sémantiques. Modèles et systèmes de gestion de la confiance. Protection de la vie privée et impacts sociopolitiques.

- Méthodes formelles en sécurité de l'information (Génie, INF 6605)

Contrôle d'accès : mécanismes, modèles (définition, spécification et vérification), limitations. Contrôle de flux d'information : mesures, spécification et analyse de flux dans un programme séquentiel. Non-interférence (spécification, analyse et limitations), généralisations de la non-interférence aux systèmes distribués (spécification, classification et analyse). Sécurité des systèmes ouverts : spécification des propriétés de sécurité, modèles d'attaques, diverses méthodes d'analyse automatisée et leurs limitations.

- Aspects électroniques de l’informatique judiciaire (Centre de formation continue, CF 150)

Intervention physique sur le média ou l’ordinateur examiné. Composants de base d’un ordinateur. Extraction de disque dur. Installation et paramétrage de systèmes d’exploitation courants. Connaissance générale des systèmes d’exploitation de serveur. Outillage d’informatique judiciaire, bloqueurs et câblages. Ateliers de pratique manuelle. Image, copie et clone des médias à l’aide de logiciels ou de machines. Mode général d’écriture d’un média (disque dur, disquette, ruban, CD). Systèmes de fichiers courants excluant NTFS. Examen d’agenda électronique et de cellulaire.

- Aspects logiciels de l’informatique judiciaire (Centre de formation continue, CF 160)

Logiciels les plus couramment utilisés en informatique judiciaire. Caractéristiques d’un bon logiciel forensic. Tests préalables à l’utilisation. Logiciel, partagiciel, gratuiciel. Type de licences et problèmes posés par certaines licences. Logiciels d’imageage judiciaire vs logiciels de gestionnaire de parc informatique (Safeback, FTK Imager, Replica et consorts Vs Ghost, DriveImage et similaires). Hashage physique et logique de média informatique. Éditeurs hexadécimaux (Disk editor et WinHex). Lecteurs d’image judiciaire de média (Encase, FTK, X-Ways et les joueurs mineurs). Casseurs de mot de passe (PRTK, DNA, Elcomsoft et les joueurs mineurs). Lecteurs de base de données comptables (WinIDEA, Drill). Gratuiciels d’informatique judiciaire.

- Preuve numérique en mode console (Centre de formation continue, CR 210)

Systèmes d'exploitation offrant un mode console. Mode console exploitable par les usagers et les administrateurs. Commandes de base et avancées. Port, descripteur, allocation de mémoire. Création d'un script. Mise en réseau. Montage sécuritaire (judiciaire) de média. Création d'un pilote. Examen sécuritaire et extraction d'information. Mode console disponible lorsque le système d'exploitation est exécuté en mode graphique. Commandes remplaçant les fonctions de l'interface graphique.

- Sécurité informatique (Génie, INF 4420A)

Définition, portée et objectifs de la sécurité informatique. Méthodologie d'analyse et de gestion du risque. Éléments de cryptographie et de cryptanalyse. Algorithmes de chiffrement à clé privée et à clé publique. Fonctions de hachage cryptographique. Signatures numériques. Gestion des clés et infrastructures à clés publiques. Sécurité des logiciels. Vulnérabilités typiques et techniques d'exploitation. Logiciels malicieux et contre-mesures. Sécurité des systèmes d'exploitation. Mécanismes d'authentification, contrôle d'accès et protection de l'intégrité. Modèles de gestion du contrôle d'accès. Sécurité des bases de données et des applications Web. Sécurité des réseaux. Configuration sécuritaire. Coupe-feux, détecteurs d'intrusions et serveur mandataire. Protocoles de réseaux sécurisés. Organisation et gestion de la sécurité informatique. Acteurs et types d'interventions. Normalisation et organismes pertinents. Cadre légal et déontologique.

- Sécurité des réseaux fixes et mobiles (Génie, INF 8402)

Sécurité des réseaux informatiques fixes et mobiles. Normes de sécurité des réseaux. Sécurité des technologies et des protocoles utilisés dans les réseaux informatiques fixes : réseaux Ethernet, réseaux TCP/IP (Transport Control Protocol/Internet Protocol) et particularités des réseaux IP. Sécurité des technologies et des protocoles utilisés dans les réseaux informatiques mobiles incluant les réseaux ad hoc, les réseaux de capteurs et les réseaux téléphoniques mobiles. Sécurité du système IMS (Internet Multimedia Subsystem) et des réseaux pair-à-pair. Technologies de sécurité des réseaux : réseaux privés virtuels et les réseaux locaux virtuels.

- Projet intégrateur en sécurité en mobilité (Génie, INF 4970)

Conception et réalisation en équipe d'applications mobiles en considérant les aspects de sécurité informatique. Utilisation des notions et des méthodes acquises dans la Concentration en sécurité et mobilité. Recours à une méthodologie de conception et de gestion nécessaire pour la réalisation d'applications mobiles sécuritaires. Attention particulière accordée à l'assurance qualité. Utilisation d'outils logiciels appropriés. Les sujets du projet peuvent provenir de l'industrie, des étudiants ou des professeurs et approuvés par le coordonnateur du cours.

- Investigation numérique en informatique (Génie, INF 8430)

Application de techniques et de protocoles d'investigation numériques pour la collecte, l'identification, la description, la sécurisation, l'extraction, l'authentification, l'analyse, l'interprétation et l'explication des données numériques contenues dans des systèmes informatiques et dans des périphériques de stockage. Capture et analyse des données volatiles, notamment des séances actives de réseaux et des processus en cours. Collecte d'informations des navigateurs Web.

- Piratage informatique (Centre de formation continue, CY 140)

Concepts de piratage informatique. Terminologie. Typologie des pirates informatiques. Cibles d'attaques. Méthodologie d'une attaque. Préparation : collecte d'information, reconnaissance, réseaux sans-fil. Attaque : Intrusion et extension de privilèges, exploitation de vulnérabilités, compromission. Conclusion : maintien d'accès, dissimulation de données et suppression des traces. Enquêtes et éléments de preuve. Tendances. Exercices et travaux pratiques en laboratoire.

- Méthodes formelles en fiabilité et sécurité (Génie, LOG 4410)

Outils mathématiques de la fiabilité des systèmes et de sécurité de l'information : structures algébriques, calculabilité, complexité de calcul, cryptographie. Modélisation des systèmes séquentiels, concurrents : réseaux de Petri (places/transitions et colorés), systèmes de transitions communicants. Spécification : logique de Hoare, logique temporelle linéaire, propriétés de sûreté de fonctionnement et de sécurité (confidentialité, authentification, anonymat, non répudiation et équité des échanges électroniques), sécurité des systèmes. Vérification : analyse des réseaux de Petri, model checking, preuves de programmes, preuves de spécifications algébriques. Applications à la sécurité : construction de programmes fiables et sécurisés, analyse des protocoles de sécurité, monitoring des activités malicieuses des systèmes logiciels.

Social Science

- Cybersécurité et cyberterrorisme (Centre de formation continue, CF 120)

La sécurité et le terrorisme sont historiquement très liés. En fait, ce duo représente les deux faces d'une même médaille ; la dynamique d'action-réaction entre les deux phénomènes est omniprésente. Depuis quelques années, de nouveaux paramètres sociaux viennent brouiller cette dynamique classique. Un de ces phénomènes est la montée des technologies de l'information et des communications (NTIC). Quel est l'impact de ces technologies sur les mesures de sécurité? Comment influencent-elles la conduite des activités terroristes? Ce cours tentera de cerner ces transformations, tout en ouvrant la réflexion sur les implications potentielles pour les autorités de sécurité.

- Cyberintimidation et société (Centre de formation continue, CF 180)

Historique de la cyberintimidation : ses différentes formes et les outils de communication préconisés. Caractéristiques de la victime et de l'offenseur. Spectre de la haine sur Internet : de la cyberintimidation à la propagande haineuse en ligne. Dépister et enregistrer les preuves de cyberintimidation. La cyberintimidation, l'éthique et le droit. Stratégies pour contrer la cyberintimidation.

- Cyberattaque: phases et défense (Centre de formation continue, CR 180)

Attaquants, motivations, provenances et types de cyberattaques. Étapes d'un processus de gestion des incidents : préparation, identification, contenir, éradication, recouvrement, amélioration du processus. Phases d'une cyberattaque : reconnaissance, balayage, exploitation des failles et obtention de l'accès, maintien de l'accès, couverture des traces. Outils et techniques de piratage utilisés lors de cyberattaque. Criminalistique informatique et aspects juridiques. Analyse de cas de cyberattaques. Détection d'attaques et moyens de défense.

Law and Administration

- Gestion de risques de l'information (Centre de formation continue, CF 170)

Ce cours s'adresse aux étudiants qui désirent développer des connaissances de base dans la gestion et l'analyse des risques de sécurité de l'information. À travers une revue des principales méthodologies de gestion et d'analyse des risques, l'étudiant acquerra une compréhension des processus, des méthodes et des outils d'analyse. Devant des cas pratique et des faits historiques, l'étudiant prendra connaissance de l'importance de la gestion de risques pour assurer la confidentialité, l'intégrité et la disponibilité de l'information. Les enjeux actuels en matière de gestion des risques dans le contexte de la sécurité de l'information, des technologies et de la cybercriminalité seront présentés.

- Internet et responsabilité civile (Centre de formation continue, CY 240)

Présentation des problématiques juridiques et civiles sur Internet. Législations applicables au Québec et Canada. Droit applicable et tribunaux compétents. Propriété intellectuelle - droits d'auteur, marques de commerce (noms de domaine), brevets. Droit à la vie privée. Protection des renseignements personnels. Politiques de vie privée et de renseignements personnels. Droit à la vie privée au travail. Politiques d'utilisation de l'Internet et des outils informatiques. Liberté d'expression, diffamation et respect de la réputation. Responsabilité civile. Responsabilité des intermédiaires techniques. Sécurité et preuve juridique sur Internet. Analyse de cas d'application de nature juridique.

- Gestion de la sécurité de l'information (Centre de formation continue, CR 110)

Tendances en sécurité. Contrôle d'accès, sécurité applicative, plan de continuité d'activités et de restauration en cas de désastre. Cryptographie, sécurité de l'information et gestion du risque. Droit, règlements, conformité et investigations. Sécurité des opérations, sécurité physique (environnementale), modèles de sécurité informatique, sécurité des télécommunications et des réseaux. Politiques de sécurité, standards et lois.

- Acquisition et analyse de preuve numérique (Centre de formation continue, CF 140)

Laboratoire d'informatique judiciaire et kit opérationnel. Enquête privée vs policière. Enquête préliminaire. Types d'autorisation judiciaire. Obtention de l'autorisation judiciaire. Planification de l'exécution de l'autorisation judiciaire. Filet de protection et mesures de sécurité personnelle. Exécution de l'autorisation judiciaire : Avant l'entrée, entrée sur les lieux, évaluation des lieux et planification de la journée, examen des médias, protection logique et physique lors de l'examen, base de décision de saisir, protection des effets saisis, après la saisie avant le départ des lieux. Remise en opération : imager et cloner. Traitement de la preuve et extraction : Imager cloner ou copier. Mise à la disposition de l'enquêteur. Calendrier de preuves. Étapes d'un procès. Présentation de la preuve à la Cour et logiciels de présentation. Numérisation de la preuve documentaire papier. Cour électronique. Éthique et étiquette.

- Enquête de piratage informatique avancé (Centre de formation continue, CR 220)

Techniques avancées utilisées en piratage informatique. Reconnaissance, attaques, évasion. Piratage psychologique moderne. Techniques d'enquêtes avancées de piratage informatique. Enquête privée ou policière. Stratégies d'analyses et d'enquêtes. Journalisation des serveurs. Outils et techniques d'analyses de journaux et de programmes malveillants. Différents outils d'analyses et conception de ses propres outils. Synthèse, rapports et expertise judiciaire.

- Gestion de risques de l’information (Centre de formation continue, CF 170)

Ce cours s’adresse aux étudiants qui désirent développer des connaissances de base dans la gestion et l’analyse des risques de sécurité de l’information. À travers une revue des principales méthodologies de gestion et d’analyse des risques, l’étudiant acquerra une compréhension des processus, des méthodes et des outils d’analyse. Devant des cas pratique et des faits historiques, l’étudiant prendra connaissance de l’importance de la gestion de risques pour assurer la confidentialité, l’intégrité et la disponibilité de l’information. Les enjeux actuels en matière de gestion des risques dans le contexte de la sécurité de l’information, des technologies et de la cybercriminalité seront présentés. L’étudiant développera les compétences pour identifier, évaluer et traiter les risques dans ce contexte.

- Enquêtes sur les crimes virtuels (Centre de formation continue, CY 150)

Déplacement partiel de la criminalité traditionnelle. Statistiques officieuses et officielles. Modèles d'intervention dans les services policiers : généralistes vs spécialistes. Création d'une unité spécialisée en cybercriminalité : logiciels, équipements, ressources humaines, gestion du travail. Défis et obstacles rencontrés par les enquêteurs. Étapes d'une enquête en matière de cybercriminalité. Identification, cueillette, conservation et présentation des éléments de preuve. Agents d'infiltration. Théories criminologiques, veille stratégique et cybercriminalité. Des laboratoires permettront de consolider les connaissances acquises par les étudiants en simulant la réalisation d'enquêtes sur des problématiques contemporaines en matière de cybercriminalité.

- Introduction à la preuve numérique (Centre de formation continue, CF 110)

Concepts de preuve numérique. Terminologie. Typologie de la preuve numérique. Catégories de preuve numérique. Utilisation de dispositifs électroniques et commission d'un crime. Les supports de stockage. Les endroits cibles. Préparation, collecte d'information, reconnaissance, réseaux sans-fil. La perquisition électronique. Modalités de recueil. Méthodologie de travail. Copie judiciaire intégrale. Agents d'infiltration. Présentation des éléments de preuve numérique. Interprétation de la preuve numérique. Contre-expertise. Dissimulation de données et suppression des traces. Processus judiciaire et éléments de preuve. Phénomène mondial. Tendances.

- Cybercriminalité, enquête policière et droit (Centre de formation continue, CY 160)

Introduction générale aux grands principes en matière de droit criminel. Les infractions rattachées à la cybercriminalité. La procédure permettant aux policiers d'enquêter dans le cyberespace et sur le terrain. Les grands principes en matière de preuve informatique. Les sentences et autres sanctions particulières à la cybercriminalité. Les développements législatifs à venir en matière de cybercriminalité et d'accès légal.

- Introduction à la criminalité informatique (Centre de formation continue, CY 100)

Introduction à Internet. Historique de l'intervention policière face à la cybercriminalité. Principaux acteurs publics, parapublics et privés. Loi de police et les niveaux de services. Revue des notions informatiques de base. Sécurité informatique, perspectives théoriques. Description des usages problématiques et criminels. Impacts économiques et sociaux de la cybercriminalité. Activités à caractère sexuel sur Internet : une perspective pratique. Cyberespace perspective d'avenir. Exercices et travaux pratiques en laboratoire.

- Prévention de la cybercriminalité (Centre de formation continue, CY 201)

Historique des programmes de prévention Internet existants et leurs évaluations. Notions de base en matière de prévention. Techniques d'évaluation de l'information en ligne. Évaluation des logiciels de filtrage de contenus illicites et préjudiciables. Enjeux, avantages et inconvénients reliés à la mise en place d'un programme de prévention. Étapes pour développer un programme de prévention; de l'analyse des besoins à l'évaluation du programme. Compétences à développer pour former des internautes avisés et responsables.

- Psychopathologie de la cybercriminalité (Centre de formation continue, CY 210)

Structure et développement de la personnalité. Étude des troubles mentaux associés à la cybercriminalité : troubles délirants, troubles sexuels, troubles de la personnalité. Réactions subjectives des intervenants et mécanismes de soutien face à la cybercriminalité. Analyses de cas : hacking, leurre, fraude, pornographie infantile. Préparation des enquêteurs à l'interrogatoire d'un cybercriminel.

- Psychopathologie de la cybercriminalité II (Centre de formation continue, CY 230)

Mise en application du cours CY210 à l'aide d'études de cas. Bref rappel des notions théoriques sur les troubles mentaux associés à la cybercriminalité. Analyse psychoclinique de cas de cybercriminalité à partir d'enregistrements vidéographiques d'entrevues d'évaluation clinique avec des cybercontrevenants reconnus coupables de délits commis par le truchement de l'Internet (hacking, leurre, fraude, pornographie infantile, etc.). Analyse de processus d'enquêtes policières portant sur des individus soupçonnés de cybercriminalité contre des enfants ou de rapt d'enfants. Analyse séquentielle des réactions psychologiques des intervenants dans ces processus d'enquêtes.

- Techniques d'entrevues (Centre de formation continue, CY 250)

Bref rappel des notions théoriques et analyses sur les troubles mentaux associés à la cybercriminalité. Revue des différentes formes d'entrevues. Spécificités des entrevues d'enquête policière ou de sécurité. Apprentissage des techniques d'entrevues d'investigation dans un travail d'enquête selon différents profils de personnalité de cybercriminels. Planification du déroulement d'entrevues d'enquête. Réalisation d'entrevues d'enquête et analyse de leurs contenus. Maîtrise des réactions émotionnelles (transférentielles) des intervieweurs lors du déroulement des entrevues.

- Enquêtes sur les délits informatiques (Centre de formation continue, CY 300)

Démonstrations et mise en pratique par des études de cas, des techniques et étapes d'enquêtes policières pour résoudre un acte criminel commis par l'entremise d'Internet. Loi de police et les niveaux de services. La coordination des dossiers d'enquêtes. Description des usages problématiques et criminels. Les lois et jurisprudences. Les infractions rattachées à la cybercriminalité. Techniques d'interrogatoires.

- Cyberfraude (Centre de formation continue, CF 100)

Historique de la cyberfraude. Introduction et revue des méthodes utilisées : falsification, détournement, divulgation, extortion, arnaque, etc. Évolution des techniques : courriel, espiogiciel, botnet, vol d'identité, hameçonnage, etc. Économie de la cyberfraude. Valeur économique de la sécurité. Impact sur la réputation des entreprises et sur la confiance des consommateurs : perceptions et réalité. Modèle de confiance et risque de réputation. Étude de cas des environnements favorables à la cyberfraude : banques en ligne, commerce électronique, encans, jeux en ligne, etc. Hameçonnage : présentation des techniques et exemples pratiques. Revue des mesures de protection, de détection et de dissuasion. Introduction aux mécanismes d'authentification. Introduction aux notions de gestion de risque et de droit supportant la prévention de la cyberfraude.

HEC Montréal

Computer Science

- Gestion du risque, contrôle et sécurité du commerce électrionique (Commerce et affaires électroniques, 4-970-02)

Au cours des dernières années, le commerce électronique a connu un essor considérable. Toutefois, limplantation du commerce électronique dans les organisations comporte certains risques qu'il ne faut pas négliger. Par conséquent, il est essentiel que les personnes impliquées dans ce type de projet soient conscientes de ces risques et qu'elles disposent d'outils adéquats pour prévenir, détecter et corriger les événements indésirables. Elles doivent également être en mesure de s'assurer de la pertinence et de l'efficacité des contrôles mis en place. Misant sur les connaissances déjà acquises dans le cadre des autres cours du programme, ce cours permettra aux étudiants d'acquérir les connaissances spécifiques à la gestion du risque inhérent au commerce électronique qui les aideront à : 1. Bien saisir l'importance de la gestion du risque ; 2. Se familiariser avec un modèle de gestion du risque; 3. Identifier les risques et les conséquences possibles ; 4. Déterminer les contrôles appropriés pour une gestion adéquate du risque ; 5. Connaître les techniques relatives à la vérification des contrôles en place ; 6. Être en mesure d'analyser des situations afin de déterminer un programme de gestion du risque approprié.

Law and Administration

- Gestionnaire et la sécurité informatique (Gestion des affaires electroniques, 30-776-04)

Qu'est-ce qui affecte 90% des entreprises et cause 17 milliards de dollars de dommages chaque année? L'absence de sécurité informatique. Les technologies de l'information n'ont jamais été à l'abri des attaques. Aujourd'hui, plus que jamais, les gestionnaires, voulant tirer le maximum des technologies, font appel à des architectures ouvertes. De telles architectures, bien que susceptibles de livrer des bénéfices substantiels, comportent aussi des risques graves. Les médias abondent d'histoires relatant les événements liés à une attaque informatique. Celles-ci sont toutes aussi monstrueuses les unes que les autres. Compte tenu de l'ampleur de la fréquence du phénomène, les gestionnaires saisis par cette problématique sont souvent démunis.

- Gouvernance et gestion des risques de la sécurité de l'information et des systèmes (Technologies de l'information, 30-715-12)

Ce premier cours du certificat en analyse de la sécurité de l’information et des systèmes offre une vue d’ensemble du domaine de la sécurité de l’information et des systèmes, en définit les grands processus et les acteurs et présente les cadres de gestion de la sécurité de l’information principalement utilisés par les entreprises. Il permet ainsi de définir le contexte organisationnel général dans lequel se mettent en œuvre les actions et les mesures visant à assurer la sécurité de l’information et des systèmes.

- Exploitation de la sécurité de l'information et des systèmes (Technologies de l'information, 30-719-12)

Ce cours permettra à l'analyste en sécurité de l'information et des systèmes de se familiariser avec les divers processus de gestion d'un centre d'exploitation de la sécurité et avec les outils technologiques utilisés. Un regard plus pointu sera porté sur les processus essentiels de l'exploitation, notamment le contrôle des accès (protéger), la gestion des évènements (détecter) et la gestion des incidents (réagir). Le cours se termine par le choix des indicateurs permettant de mesurer la performance de l'exploitation de la sécurité dans une optique d'amélioration continue et de réponse aux besoins d'affaires.

- Atelier de préparation à la certification CISSP (Technologies de l'information, 30-707-12)

Le contenu de cet atelier préparatoire est aligné sur les dix domaines de connaissance définis par l'(ISC)2 pour réussir l'examen et obtenir la certification CISSP, soit : Gouvernance de la sécurité de l'information et gestion des risques; Télécommunications et sécurité du résea;u Chiffrement; Sécurité des applications; Contrôles des accès Lois, règlements, enquêtes et conformité; Design d'architecture et sécurité; Sécurité de l'environnement physique; Exploitation de la sécurité de l'information et des systèmes; Continuité des activités et plans de reprise après sinistre.

- Sécurité physique de l'information et des systèmes et initiation à la criminalistique (Technologies de l'information, 30-716-12)

Objectifs spécifiques: Comprendre la place de la sécurité physique dans le processus de sécurisation d’un site; Connaître la terminologie et les principaux concepts des diverses disciplines en lien avec la sécurité physique; Être en mesure d’appliquer les principes de la prévention de la criminalité par l’aménagement du milieu (PCAM); Être capable de définir ces besoins comme client; Développer un regard critique sur la sécurité en général pour être capable de briser les paradigmes.

- Cadres réglementaires et de contrôle de la sécurité de l'information et des systèmes (Technologies de l'information, 30-708-12)

Plus que jamais, les entreprises manipulent et stockent des quantités faramineuses de données concernant leurs clients, leurs employés et leurs partenaires d'affaires. Les médias regorgent de nouvelles concernant les crimes informatiques et les exploits des pirates du Web et des « hacktivistes ». Devant cette escalade sans cesse croissante d'incidents, les gouvernements ont réagi en mettant en place des lois afin d'encadrer les comportements et actions des entreprises, des organismes publics, des individus et des criminels (propriété intellectuelle, secrets industriels, protection des renseignements personnels, etc.) et certaines industries se sont prises en main étant donné les sommes astronomiques perdues (le plus bel exemple étant l'industrie des cartes de crédit avec la norme PCI DSS). Dans le premier cas, le but est de « policer » le far west virtuel afin de ne pas être des victimes sans défense. Dans le deuxième cas, le but est plutôt de diminuer les pertes financières et de soutenir et de renforcer un système qui, somme toute, repose sur la confiance. Les professionnels de la sécurité de l'information doivent être au fait du système juridique, réglementaire et normatif entourant la sécurité de l'information et les crimes informatiques qui s'appliquent à leur contexte d'affaires. Ils doivent être sensibilisés aux devoirs et responsabilités de leur entreprise quant aux données qu'elle recueille, conserve et utilise autant de leurs partenaires externes que sur ses propres employés et connaître les mesures à mettre en œuvre pour se protéger. Ils doivent aussi comprendre les obligations de l'organisation lorsque des tiers sont impliqués et connaître les différents cadres de contrôle généralement adoptés par les organisations. Au total, l'analyste doit comprendre le contexte dans lequel il œuvre en matière de sécurité de l'information et être en mesure d'évaluer le moment où des ressources spécialisées (comme le service juridique ou les services professionnels d'un avocat spécialisé dans le domaine) sont requises, moment où les connaissances de base acquises leur permettront de jouer le rôle d'intermédiaire.

- Sécurité des applications (Technologies de l'information, 30-717-14)

Les organisations dépendent de leurs applications pour la bonne conduite de leurs affaires et les utilisent dans des contextes toujours plus éclatés et dans une logique de partage d'information avec un nombre toujours plus grand de partenaires. De toutes les menaces, ce sont celles liées aux applications qui préoccupent le plus les spécialistes en sécurité. En effet, une étude de Frost & Sullivan[1], réalisée en 2010 auprès de 10 413 professionnels de la sécurité de l'information, dévoile que 73 % d'entre eux place la vulnérabilité des applications en tête de liste de leurs préoccupations. Malgré cela, trop souvent les activités et les réflexions liées à la sécurité des applications sont absentes des méthodologies traditionnelles de développement. Pour qu'un système soit optimal, tant du point de vue de ses fonctionnalités que de sa sécurité, il est souhaitable de lier ces deux catégories d'exigence, du moment de la conception de l'application jusqu'au moment de sa mise en service. Cette approche est préférable à celle généralement en vigueur qui préconise la mise à niveau continue de correctifs qui ont pour effet de laisser des « trous » que les cybercriminels auront vite fait d'exploiter. Dans ce cours, nous démystifierons les pratiques d'excellence à mettre en œuvre pour optimiser la sécurité des applications en fonction du contexte spécifique de leur utilisation, donc en adoptant une vision holistique d'évaluation et de gestion des risques. L'accent est mis sur le cycle de développement sécuritaire, sur les façons d'utiliser les technologies (applications et tests) pour permettre de déceler les vulnérabilités applicatives et sur les méthodes de détection et de contrôle de ces vulnérabilités.

- Sécurité de l'infrastructure (Technologies de l'information, 30-718-12)

Aujourd'hui, plus que jamais, les entreprises voulant exploiter au maximum le potentiel des technologies de l'information font appel à des infrastructures ouvertes. Une telle orientation, bien que susceptible de livrer des bénéfices économiques substantiels, comporte aussi des risques importants qu'il faudra bien analyser. Les attaques sur les différentes composantes de l'infrastructure technologique des entreprises (commutateurs, systèmes d'exploitation, portables, téléphones cellulaires, applications, etc.) ainsi que leurs conséquences parfois dévastatrices sont légion. Afin de bien jouer son rôle, l'analyste en sécurité de l'information et des systèmes doit acquérir une solide compréhension des composants d'une infrastructure et de leur fonctionnement, de leurs vulnérabilités et des processus et technologies, autant le matériel que les applications, à utiliser pour les protéger. Ce cours permettra au futur analyste d'acquérir les connaissances lui permettant de choisir et d'exploiter les multiples technologies à sa disposition afin de développer une solide ligne de défense assurant la protection de l'infrastructure technologique de l'entreprise. APPROCHE PÉDAGOGIQUE : Ce cours adopte à la base une approche magistrale. Toutefois, des démonstrations et des exercices à l'aide d'applications variées de gestion de la sécurité de l'infrastructure seront intégrés au contenu de chacune des séances.

McGill University

- Cryptography and Data Security (Computer Science, COMP 547)

This course presents an in-depth study of modern cryptography and data security. The basic information theoretic and computational properties of classical and modern cryptographic systems are presented, followed by a cryptanalytic examination of several important systems. We will study the applications of cryptography to the security of systems.

- Quantum cryptography (Computer Science, COMP 649)

Review of the basic notions of cryptography and quantum information theory. Quantum key distribution and its proof of security. Quantum encryption, error-correcting codes and authentication. Quantum bit commitment, zero-knowledge and oblivious transfer. Multiparty quantum computations.

- Advanced cryptography (Computer Science, COMP 647)

Information theoretic definitions of security, zero-knowledge protocols, secure function evaluation protocols, cryptographic primitives, privacy amplification, error correction, quantum cryptography, quantum cryptanalysis.

- Language-based security (Computer Science, COMP 523)

State-of-the-art language-based techniques for enforcing security policies in distributed computing environments. Static techniques (such as type- and proof-checking technology), verification of security policies and applications such as proof-carrying code, certifying compilers, and proof-carrying authentication.

- Computer Network and Internet Security (School of Continuing Studies, CCS2 510)

Computer Science (CCE) : Basic principles, design and performance of computer networks. Theory and technology, including network security models, cryptography protocols and standards, network security threats and types of attacks, security counter-measure strategies and tools, firewalls, access control and platform-specific security issues.

- Information Security (Information Studies, Faculty of Arts, GLIS 629)

Introduction to information security. Topics include basic concepts of confidentiality, integrity, and availability; security threats; malware; operating systems security; access control; network security (encryption, decryption, passwords and digital signature);security policies and practices; risk assessments; common criteria; privacy threats and protection techniques; cybercrime and cyber forensics.

- Information Systems Security (Software Development/Systems Analysis and Design, School of Continuing Studies, CMIS 422)

Management Information Systems: Fundamental concepts relating to the design of secure information systems. Identification and assessment of security risks at the application, network, and physical levels. Use of cryptography and other techniques to provide necessary level of security.

TÉLUQ

Computer Science

- Réseaux et sécurité informatique (Science et Technologie, INF 1165)

Définition des principaux concepts de sécurité informatique. Introduction à la cryptographie comme moyen de protéger l'information. Description et répertoire des types d'attaques auxquelles un réseau d'entreprise peut faire face. Analyse des risques. Définition de la politique de sécurité (recueil de règles, normes et standards). Méthodes de protection et solutions techniques contre les attaques. Introduction aux missiles virtuels de destruction massive. Stratégie de sécurité, procédures et outils de contrôle : capture de paquets, logiciels de capture et utilisation des pare-feu. Éléments de la sécurité des réseaux sans fil.

Law and Administration

- Gestion de la sécurité des technologies de l'information (Sciences de l'administration, ADM 6046)

Permettre à l'étudiant de développer une vision globale de la sécurité de l'information sur le plan de la gestion. Connaître les différentes composantes d'une politique de sécurité, les meilleures pratiques en sécurité et les actions nécessaires pour assurer une protection suffisante et contrôlée de l'ensemble des actifs informationnels. À la fin de ce cours, l'étudiant aura toutes les connaissances nécessaires pour superviser la gestion de la sécurité de l'information dans une organisation, analyser l'état de la sécurité de l'information et proposer des mesures pour répondre à ses besoins de sécurité.

- Gestion des risques en affaires électroniques (Sciences de l'administration, ADM 6030)

Fournir une large compréhension des risques associés à la sécurité des technologies de l'information et aux enjeux légaux et éthiques du commerce électronique dans un contexte d'affaires. Plus précisément, permettre à l'étudiant d'atteindre les objectifs suivants : connaître les fondements et les concepts clés de la sécurité de l'information en contexte d'affaires électroniques; prendre des décisions en matière de politiques de la sécurité de l'information en tenant compte des principales lignes directrices et des éléments à considérer; évaluer les enjeux légaux et éthiques des risques associés à la gestion de l'information en affaires électroniques; évaluer les bénéfices, les contraintes, les risques et les enjeux de la gouvernance de la sécurité de l'information; choisir les logiciels qui permettent de sécuriser les transactions sur Internet; examiner les implications des décisions concernant la sécurité des données personnelles et d'affaires sur la responsabilité organisationnelle et la confiance du public; choisir différents types de transfert de risques dans les contrats de cyberassurances; mesurer les risques associés à la sécurité des données à l'aide de critères valables et être au fait des différentes approches pour gérer la sécurité des technologies de l'information.

Université de Montréal

Computer Science

- Cryptologie: théorie et applications (Informatique et de recherche opérationnelle, IFT 6180)

Historique et définitions. Cryptographie et cryptanalyse. Théorie de l'information. Cryptographie conventionnelle, à clefs publiques, probabiliste et quantique. Génération pseudo et quasi aléatoire. Applications diverses.

- Sécurité informatique (Informatique et de recherche opérationnelle, IFT 6271 and IFT 3275)

Confidentialité et intégrité des données. Protection des réseaux et du commerce électronique. Clefs publiques et les tiers de confiance. Méthodes d'authentification. Coupe-feu. Gestion des mots de passe. Évaluation et gestion des risques et sécurité.

- Sécurité des systèmes informatiques (Informatique et de recherche opérationnelle, IFT 2830)

Introduction à la sécurité informatique. La sécurité d'un ordinateur personnel. Protocoles et cryptographie. Applications internet. Protection réseau. Programmation sécurisée.

- Nouvelles technologies et crime (Criminologie, CRI 6234)

Impacts des nouvelles technologies sur la criminalité existante et émergente, ainsi que sur la sécurité des individus et des organisations. Bilan des technologies utilisées par les institutions de contrôle social.

Social Science

- Criminalistique et information (Criminologie, CRI 6861)

Séminaire traitant de la collecte et de l'exploitation des traces numériques qui résultent d'un comportement délictueux au cours duquel un système électronique de traitement de l'information a été utilisé.

- Criminalistique et cybercriminalité (Criminologie, CRI 6864)

Protection des données et cybercriminalité. Risques et opportunités liés à l'utilisation des technologies d'information et de communication par les forces policières. Remarques: Enseigné uniquement à Lausanne.

- Criminalité informatique (Criminologie, CRI 3950)

Présentation des principales formes de criminalité informatique. Usages problématiques et criminels d'Internet. Législation et intervention policière dans le cyberespace. Impacts des nouvelles technologies sur le milieu criminel.

Law and Administration

- Droit de la protection des données personnelles (Droit, DRT 6913)

Normes québécoises et canadiennes concernant la protection des informations personnelles; règles de conservation et de communication; recours administratifs et judiciaires.

Université de Sherbrooke

Computer Science

- Sécurité et cryptographie (Génie, IFT 606)

Concepts de base de la sécurité informatique. Confidentialité. Authentification. Intégrité. Contrôle des accès. Cryptographie. Signature électronique. Certificats. Gestion de clés. Attaques et parades. Virus. Architectures. Coupe-feu. Réseaux virtuels privés. Politiques de sécurité. Méthodologies, normes et analyse de risques.

- Projet d'intégration en sécurité logicielle (Génie, GEI 776)

Cibles de formation : planifier l'analyse de la sécurité d'un système, puis mettre en oeuvre un plan de sécurisation d'un système informatique et en valider le résultat. Contenu : choix d'un système à évaluer (application régulière, application web, serveur, réseau interne, postes de travail, appareils autonomes, etc.). Choix des outils d'analyse et de test pour repérer les vulnérabilités et production d'un rapport de planification. Exécution du plan d'évaluation et de correction de la sécurité d'un système. Repérage des problèmes de sécurité, conception des correctifs à apporter. Mise en oeuvre des solutions proposées et validation; présentation d'un rapport et défense devant un jury.

- Projet d'intégration en sécurité informatique (Génie, GEI 775)

Cibles de formation : planifier l'analyse de la sécurité d'un système, puis mettre en oeuvre un plan de sécurisation d'un système informatique et valider le résultat. Contenu : choix d'un système à évaluer (application régulière, application web, serveur, réseau interne, postes de travail, appareils autonomes, etc.). Choix des outils d'analyse et de test pour identifier les vulnérabilités et production d'un rapport de planification. Exécution du plan d'évaluation et de correction de la sécurité d'un système. Identification des problèmes de sécurité, conception des correctifs à apporter. Mise en oeuvre des solutions proposées et validation; présentation d'un rapport et défense devant un jury.

- Concepts de cryptographie et de sécurité (Génie, GEI 774)

Cibles de formation : maîtriser les diverses techniques de cryptage, identifier les vulnérabilités d'un système et choisir les techniques appropriées répondant à des critères spécifiques de sécurité. Contenu : cryptographie : chiffrement par flux, par bloc; clés symétriques, standards DES , AES ; clés privées, clés publiques, RS A, Diffie-Hellman; introduction à la théorie des nombres. Sécurité : notions de sécurité et de violation, contrôle d'accès, mots de passe; vulnérabilités, dépassement de tampons.

- Sécurité informatique et cryptographie (Génie, GIF 630)

Cible de formation : mettre en oeuvre une technique de cryptage appropriée répondant à des critères spécifiques de sécurité. Contenu : cryptographie : protocoles et algorithmes, codes sécuritaires, clés privées, clé publique et signatures numériques. Standard DES. Sécurité : notions de sécurité et de violation, modélisation et mise en oeuvre du contrôle d'accès. Analyse des risques et planification de la sécurité. Sécurité des systèmes d'exploitation et des bases de données.

- Sécurité et contrôle des TI (Génie, GIS 358)

Politique de sécurité, modèles de gestion du risque, forces et faiblesses des systèmes de sécurité, contrôles informatiques généraux, procédures et contrôles internes d'entreprise, pannes et récupération, plan de contingence. Aspects légaux liés à la sécurité et à la confidentialité. Visions de l'utilisatrice ou utilisateur, de l'informaticienne ou informaticien et de la vérificatrice ou du vérificateur. Approche par cas.

- Introduction à l'investigation numérique (Génie, GEI 773)

Préparation préventive des systèmes, journalisation, éléments névralgiques (systèmes de fichiers, répertoires sensibles, communication réseau, clés et disques USB, mémoire), aseptisation, analyse sans modification, outils logiciels.

- Sécurité web (Génie, GEI 772)

Vulnérabilités côté client (XSS, plugiciels malveillants, usurpation de clics). Vulnérabilités côté serveur (déni de service, injection SQL, réutilisation de paquets). Techniques de protection (infrastructure d'authentification, choix des protocoles, techniques de filtrage). Sécurisation des échanges client-serveur.

- Programmation sécurisée (Génie, GEI 771)

Analyse et modélisation des risques d'une application, identification des types de failles. Mesures de contingence : appels à bannir, protection de la pile, protection des communications, protection des données, etc. Niveau de protection des langages. Pièges de la cryptographie (générateurs de nombres aléatoires, taille et réutilisation de clés, temps de réponse). Méthodes de test (carré de sable, virtualisation, environnements d'aide au test, tests aléatoires).

- Sécurité des systèmes informatiques (Génie, GEI 762)

Étapes d'une intrusion : reconnaissance, surveillance, exploitation, nettoyage. Classes et types d'exploitation : virus, vers, rootkits, botnet, portes dérobées, déni de service, mascarade, escalade de privilèges. Méthodes d'exploitation : dépassement de tampon et tas, failles de protocoles, etc. Signes d'une reconnaissance et de perte d'intégrité du système (journaux, fichiers, etc.). Protection active (installation de guet-apens, etc.).

- Télématiques et protocoles sécurisés (Génie, GEI 761)

Protocoles de sécurité selon les couches de la pile TCP/IP. Mécanismes de sécurité intrinsèques aux protocoles de sécurité. Conception d'applications sécuritaires. Intégration sécuritaire de fonctionnalités de tierces parties dans le développement d'applications.

- Techniques avancées de cryptographie (Génie, GEI 760)

Méthodes d'encryptage à clé privée El Gamal et à courbes elliptiques. Méthode d'encryptage symétrique AES (Rijndael), ainsi que les méthodes concurrentes (Serpent, Twofish, Blowfish). Techniques de calcul rapide applicables aux méthodes d'encryptage à clé privée (Karatsuba, Toom-Cook, Montgomery, etc.). Preuves à divulgation nulle de connaissance. Techniques de factorisation modernes (Pollard, crible quadratique, introduction au crible à champs de nombres).

Law and Administration

- Gestion de la sécurité de l'information (Informatique de la Santé, ISA 405)

Cibles de formation : développer un plan de gestion des incidents dans le cadre d'un système d'information médical et en assurer la maintenance. Contenu : sinistres et incidents majeurs liés au domaine des soins de santé et des services sociaux.

- Analyse et gestion des risques en santé (Informatique de la Santé, ISA 404)

Cibles de formation : créer un plan directeur pour gérer les risques liés aux technologies de l'information en fonction des objectifs d'un établissement de soins de santé et de services sociaux et en assurer le suivi. Contenu : gestion des risques : concepts, démarche, ateliers, outils, exemples; application de l'analyse de risques dans le domaine de la santé; application de l'analyse de risques dans la sécurité des TI du domaine de la santé; application de l'analyse de risques dans les projets des établissements de santé et de services sociaux; application de l'analyse de risques dans la continuité des affaires. Élaboration d'un plan directeur.

- Accès et protection des données personnelles (Droit, DRT 588)

Introduction aux notions de vie privée et de renseignements personnels. Instruments nationaux et internationaux encadrant le traitement (de la collecte à la destruction) des renseignements personnels - secteurs public et privé. Application au secteur de la santé, au commerce électronique, aux prestations électroniques de service, au travail. Le rôle des autorités de contrôle.

- Gouvernance de la sécurité des actifs informationnels (Administration, DAT 813)

Cibles de formation : connaître les principes de la sécurité de l'information et de la protection des actifs informationnels tels que les menaces, les risques, les vulnérabilités et les contrôles. Connaître également l'ensemble des activités nécessaires pour assurer une protection suffisante et contrôlée de l'ensemble des actifs informationnels. Contenu : les éléments clés de la gestion de la sécurité de l'information; les approches de gestion de risques en matière de sécurité de l'information; la sécurité des infrastructures d'une organisation; les meilleures pratiques en sécurité de l'information (ISO 27000).

Université du Québec à Chicoutimi

- Sécurité informatique et réseaux (Informatique et mathématique, SIF 104)

Faire comprendre la problématique générale de la sécurité au niveau local et grand public. Initier à l'architecture TCP/IP. Développer les habiletés nécessaires pour gérer et configurer un environnement client-serveur sécurisé. Historique et topologie des réseaux. Survol de l'architecture TCP/IP et les couches ISO. La vulnérabilité des principaux protocoles et services TCP/IP (ex. FTP, SMTP, HTTP, ...). L'interconnexion et les algorithmes de routage. La problématique des transactions sur réseau par le commerce électronique. Mise en oeuvre d'une politique de sécurité. L'analyse de risque. Techniques et outils logiciels assurant la sécurité et la confidentialité de l'information. Impact du commerce électronique sur la sécurité. L'encryption traditionnelle (ex. codage de substitution et de transposition) et moderne. Les algorithmes à clé secrète (ex. DES, IDEA) et à clé publique (ex. RSA); les protocoles d'authentification basés sur Kerberos ou utilisant une clé partagée, publique ou distribuée par un centre. Les signatures numériques utilisant une clé secrète ou publique (ex. DSS). Les impacts sociaux de la sécurité. Analyse comparative sur la fiabilité, le risque et les exigences sur le codage et le décodage. L'impact des réseaux privés virtuels sur la sécurité. Les attaques: concept, type, protection. Le coupe-feu: concept, application. Le proxy: justification, niveau de sécurité, activation, application. Critères de sélection aux niveaux logiciel et matériel d'un serveur réseau; choix, installation, configuration et utilisation d'un serveur réseau. Gestion des services et des utilisateurs.

- Sécurité informatique (Informatique et mathématique, SIF 135)

Amener à comprendre les concepts de base de la sécurité informatique et de la protection de l'environnement de travail grâce à des logiciels et des protocoles de sécurité. Faire acquérir une approche pratique de la sécurité dans l'environnement de l'Internet. Concepts de base de la sécurité informatique. Menaces. Vulnérabilité des systèmes. Survol des technologies utilisées en sécurité informatique: cryptographie, cryptanalyse, authentification, confidentialité, codes malicieux, pare-feux, audits, détection d'intrusions, etc. Principes de base pour sécuriser un environnement réseau. La taxonomie d'attaques malicieuses sur les réseaux informatiques. Les faiblesses des protocoles réseaux. Installation et configuration des outils de sécurité réseau. Protocoles de sécurité. Sécurité du Web. Concepts de politique de sécurité pour les réseaux. Étude approfondie des technologies utilisées pour la protection des réseaux informatiques. Sécurité de commerce électronique. Modèles de sécurité des langages de programmation. Vérification des mécanismes de sécurité implantés dans une organisation donnée.

- Cryptographie (Informatique et mathématique, INF 854)

Comprendre le fonctionnement des principaux protocoles et algorithmes cryptographiques ainsi que leurs applications. Historique: Notions élémentaires de la théorie des nombres et de la théorie de la complexité; Cryptologie à clef privée et publique; Signature électronique, fonctions de hachage à sens unique; Protocole d'échange de clefs, échange de clefs; Exemples de librairie dans des langages tels que C et Python; cryptologie quantique (si le temps le permet), Cryptosystèmes à courbes elliptiques (si le temps le permet).

- Sécurité informatique (Informatique et mathématique, INF 857)

Ce cours vise à comprendre les différents problèmes de la sécurité informatique (confidentialité, intégrité, disponibilité, authentification, non répudiation) et leurs solutions dans divers environnements: local et réseau. Plus spécifiquement: Connaître les mécanismes de base qui permettent de contrôler l'accès à un système et ses ressources; développer le savoir-faire nécessaire à la sécurisation des applications d'entreprise, d'un système informatique et du réseau Internet; être capable de proposer des mesures adéquates pour éviter les attaques; familiariser les étudiants avec les commerces électroniques sécurisés; gérer la sécurité d'un système et analyser les risques. Introduction: Importance de la sécurité pour une entreprise; sécurité local et distance. Sécurité des télécommunications et d'accès: Internet, faiblesses du protocole TCP-IP, analyse de ports; Intranet, Extranet, gardes-barrière (Firewall), Proxy, VPN, IPsec. Sécurité des systèmes d'exploitation: Permissions et Log files. Confidentialité: Le cryptage; Chiffrement symétrique (DES, 3DES, AES, IDEA), Chiffrement asymétrique (clé publique-privée, RSA, ELGAMAL). Authentification: Méthodes d'authentification faibles et fortes; Mot de passe, One-Time password (S-KEY), Signature, Certificat et Biométrie. Intégrité: Chiffrement asymétrique et chiffrement symétrique, Signature numérique. Sécurité des applications et des langages de programmation: Modèle de sécurité en Java, JAAS, sécurité de code C-C++; Communications sécurisées clients-serveurs. Commerces et messageries électroniques: Messageries électroniques (SMTP, S-MIME, PGP), Commerces électroniques avec le protocole SSL, Secure Electronic Transactions (SET); transfert électronique de fonds. Méthodes de gestion de la sécurité: Déterminer l'impact de chaque actif informationnel en termes de confidentialité, d'intégrité et de disponibilité; Méthode MEHARI, Cobit, Normes ISO.

- Sécurité des applications (Informatique et mathématique, INF 333)

Faire prendre conscience des risques informatiques les plus fréquents et apprendre à maitriser les outils et les bonnes pratiques de programmation permettant de les éviter. Familiariser avec le vocabulaire et les notions fondamentales nécessaires à la compréhension des problèmes de sécurité auxquels un informaticien fait face durant sa carrière. Pourquoi la sécurité informatique est importante. Exemple de vulnérabilité. La conception sécuritaire des logiciels. Dépassements de tampon: outils et techniques de protection. Vulnérabilité de format de chaîne: représentation sur la pile des fonctions variadiques; mécanismes de détection et contremesures. Validation des entrées: injection SQL; injection de code; injection http; mécanismes de détection et contremesures. Introduction au model-checking; Analyse statique et son utilisation en sécurité: typage et sécurité des types, taint checking; assertion de sécurité, analyse de bornes. Sécurité du système d'exploitation: accès aux ressources; protection des fichiers; authentification. Tests d'évaluation de la sécurité: différence avec les tests fonctionnels; tests black-box et white-box; tests de pénétration. Les HIDS (host-bases intrusion detection systems): principes de bases; attaques par imitation. Aspects éthiques et légaux de la sécurité informatique.

- Sécurité des systèmes informatiques (Informatique et mathématique, INF 837)

Moyens pour associer la sécurité des données et des processus dans un environnement informatique. Cryptologie. Authentification. Sécurité et réseau informatique. Protocoles sécuritaires. Menaces contre le logiciel et le matériel : virus, fraudes, détournements, impostures.

- Applications réseaux et sécurité informatique (Sciences appliquées, GEI 466)

Appliquer la méthodologie propre au génie logiciel afin de développer des applications utilisant les fonctionnalités d'un réseau et améliorer la sécurité dans les échanges d'informations électroniques. Rappel sur les protocoles de communication: IP, TCP, utilisation des ports. Familiarisation aux différents langages et standards utilisés pour mettre en oeuvre des applications WEB: DHTML, XHTML, XML, Perl, Javascript, ASP, Java, Java Servlets, ActiveX, PHP. Développement d'applications utilisant ces langages. Utilisation de «cookies». Sécurité informatique: gestion du risque, cryptographie, signatures numériques, authentification, vulnérabilités, protocoles sécurisés, configuration des équipements de communication.

- Sécurité des réseaux et du Web (Informatique et mathématique, INF 135)

Amener à comprendre les concepts de base de la sécurité informatique et de la protection de l'environnement de travail grâce à des logiciels et des protocoles de sécurité. Faire acquérir une approche pratique de la sécurité dans l'environnement de l'Internet. Concepts de base de la sécurité informatique. Menaces. Vulnérabilité des systèmes. Survol des technologies utilisées en sécurité informatique: cryptographie, cryptanalyse, authentification, confidentialité, codes malicieux, pare-feux, audits, détection d'intrusions, etc. Principes de base pour sécuriser un environnement réseau. La taxonomie d'attaques malicieuses sur les réseaux informatiques. Les faiblesses des protocoles réseaux. Installation et configuration des outils de sécurité réseau. Protocoles de sécurité. Sécurité du Web. Concepts de politique de sécurité pour les réseaux. Étude approfondie des technologies utilisées pour la protection des réseaux informatiques. Sécurité de commerce électronique. Modèles de sécurité des langages de programmation. Vérification des mécanismes de sécurité implantés dans une organisation donnée.

Université du Québec à Montréal

Computer Science

- Sécurité des systèmes informatiques (Informatique, INF 8750)

Principes et concepts fondamentaux de la sécurité des systèmes informatiques. Principaux services: confidentialité, intégrité, disponibilité, authentification, non répudiation, contrôle d'accès. Typologie des attaques: fuites, modifications d'information, privations de service. Mécanismes sécuritaires modernes: systèmes de chiffrage symétriques et asymétriques; fonctions de hachage; génération pseudo-aléatoire. Protocoles sécuritaires: authentification, signature, échange et gestion de clés. Sécurité des systèmes centralisés et des systèmes répartis: politiques et modèles de sécurité; contrôle d'accès; rôles et privilèges. Sécurité des programmes: virus, chevaux de Troie. Contre-mesures: journalisation, audits; détection d'intrusion; filtrage; mécanismes de recouvrement. Analyse de risque. Éducation des usagers. Considérations légales, politiques et éthiques.

- La cryptographie, de l'Antiquité à l'Internet (Sciences, FSM 4100)

Ce cours a pour objectif de présenter la cryptographie et les principes mathématiques sous-jacents, dans une perspective historique. Il s'adresse à des étudiants sans préalable mathématique de niveau universitaire. Survol des premiers systèmes de codages et leurs contextes historiques: code de César, codes par substitution, code de Vigenère, code de Vernam, code de Playfair, code de Hill, etc. Notions mathématiques nécessaires à la description de ces codes: matrices modulo un entier, arithmétique modulaire, algorithme d'Euclide. Outils de décodage: approche probabiliste, théorie de l'information de Shannon: entropie, incertitude, information, entropie conditionnelle, système cryptographique parfait. Cryptographie moderne: systèmes à clé publique, RSA, logarithme discret. Perspectives d'avenir pour la cryptographie: aperçu de cryptographie quantique.

- Protection des réseaux informatiques (Management et technologie, MET 8330)

Ce cours vise à développer chez l'étudiant un processus de pensée critique de la sécurité des réseaux informatiques centrés sur les besoins d'affaires de l'organisation. Pour ce faire, l'étudiant devra analyser les différentes méthodologies, normes et outils de sécurité disponibles, effectuer une sélection arrimée sur les besoins organisationnels et appliquer ces mesures dans un contexte d'optimisation des ressources. Il s'agit de développer les savoirs et savoir-faire des étudiants dans le domaine des différents risques encourus par les technologies de l'information en axant la formation sur l'acquisition de connaissances et l'exercice pratique d'évaluation et de traitement des risques. Objectifs pédagogiques : - définir et expliquer les différentes normes et méthodologies de gestion et d'évaluation des risques informatiques; - définir et expliquer les principales technologies et pratiques contribuant à une réduction des risques informatiques; - appliquer un processus de gestion des risques informatiques; - acquérir et maîtriser différentes techniques de gestion, de modélisation et de résolution de problèmes propres à la gestion d'un processus, des TI et de son projet de changement. Les principaux thèmes abordés dans ce cours sont : - les principes et concepts fondamentaux des réseaux informatiques et leur architecture en vue de leur éventuelle implantation, exploitation ou intégration dans les organisations; - les principaux concepts de la sécurité informatique dans divers contextes d'utilisation, tels que dans le cas des usagers mobiles ou des organisations délocalisées; - les principaux enjeux de sécurité des réseaux informatiques filaires et sans fil; - les principes de cryptographie, de signatures numériques et d'authentification nécessaires afin de sensibiliser, sur les enjeux de la sécurité, les usagers des systèmes informatiques et d'information dans les organisations; - les types d'attaques auxquelles un réseau informatique est exposé; - les méthodes de protection et les solutions techniques contre les attaques quant aux services et aux coûts relatifs au déploiement des progiciels et/ou des infrastructures; - l'analyse des risques et la définition de la politique de sécurité (recueil de règles) en tenant compte des aspects légaux et administratifs de la sécurité.

- Réseau et sécurité des systèmes d'information (Informatique, INF 6065)

Au terme du cours, l'étudiant sera en mesure d'identifier les vulnérabilités et les risques auxquels les systèmes informatiques sont exposés, de choisir et de déployer les contre-mesures appropriées pour assurer la sécurité d'une organisation et la protéger contre les menaces internes et externes. Il sera en mesure de développer et de mettre en place une stratégie sécuritaire globale pour les ressources en technologie de l'information. Le cours vise à initier l'étudiant aux principes de sécurité des systèmes basés sur les technologies de l'information, notamment les méthodes, les pratiques ainsi que les politiques permettant d'assurer la sécurité dans les organisations y compris celles virtuelles. Le cours lui permettra de se familiariser avec les dispositifs qui servent à assurer la sécurité des ressources informatiques, de développer la capacité d'évaluer les risques d'attaques, le niveau de vulnérabilité, de proposer des solutions de protection des réseaux et des informations, de développer des habiletés permettant de déterminer et d'élaborer une véritable stratégie de sécurité conforme aux normes et exigences en matière de gestion de systèmes d'information.

- Fiabilité et sécurité informatique (Informatique, INF 4470)

Sensibiliser les étudiants aux différents aspects de la fiabilité et de la sécurité des systèmes informatiques. Introduire les techniques permettant d'assurer la fiabilité et la sécurité des processus. Fiabilité d'équipements et de logiciels. Procédures de sauvegarde et de recouvrement. Redondance. Tolérance aux défaillances et aux erreurs. Menaces à la sécurité: virus, imposteur, espion. Cryptologie. Authentification. Sécurité des systèmes répartis. Forteresse (firewall) contre intrusions. Travaux en laboratoire.

Law and Administration

- Gestion de la protection des ressources informatiques (Management et technologie, MET 3211)

Acquisition des connaissances de base dans la planification, la conception, l'implantation et l'évaluation d'un programme de protection des ressources informatiques. Identification des menaces informatiques et de leurs conséquences. Aperçu de la législation canadienne et québécoise dans le domaine. Conception d'un programme de protection de recours informatique. Mesures et techniques de protection des équipements et du personnel. Mesures d'urgence.

Université du Québec à Rimouski

- Sécurité informatique (Informatique, INF 36207)

Historique. Cibles probables et courantes. Vulnérabilités et types d'attaques. Sécurité dans les systèmes d'exploitation. Sécurité dans les bases de données, Sécurité dans les réseaux. Sécurité dans les logiciels. Cryptographie et cryptanalyse.

Université du Québec en Outaouais

- Sécurité des réseaux informatiques (Informatique et Ingénierie, INF 1443)

Démarche utilisée par un intrus pour attaquer un réseau informatique : reconnaissance, acquisition d'informations, exploitation, sécurisation d'accès, élimination des traces. Principaux outils utilisés pour analyser et attaquer un réseau : whireshark, nmap, nessus, metasptoit, etc. Vulnérabilités des systèmes Windows et Unix. Vulnérabilités des applications. Contre-mesures disponibles pour faire face aux différentes attaques réseaux. Sécurité des réseaux sans fils. Réseaux virtuels privés et leurs vulnérabilités. Ce cours comporte des séances obligatoires de travaux dirigés (TD) de deux heures par semaine.

- Analyse et conception des protocoles de sécurité (Informatique et Ingénierie, INF 6103)

Cryptographie. Protocoles de sécurité. Rôle des protocoles de sécurité dans les systèmes de communication et les systèmes distribués. Présentation de quelques protocoles existants. Propriétés de sécurité : confidentialité, authentification, anonymat, atomicité, non-répudiation, etc. Taxonomie des failles de sécurité. Langages formels pour la spécification des protocoles de sécurité CCS/CSP, SPI, BAN, SPC, etc. Techniques formelles de vérification et preuves de correction des protocoles de sécurité.

- Sécurité informatique et méthodes formelles (Informatique et Ingénierie, INF 6233)

Problèmes de la sécurité dans les logiciels et intergiciel. Formalismes algébriques et logiques pour la description des systèmes et des politiques de sécurité. Automates d'édition. Techniques formelles de renforcement de politiques de sécurité dans les systèmes. Renforcement par Monitorage. Renforcement par réécriture de programmes. Classes de propriétés de sécurités : sûreté, vivacité, « renewal », etc.

- Sécurité des données (Informatique et Ingénierie, INF 6005)

Risques et menaces à la sécurité des données. Sécurité et systèmes d'exploitation. Analyse des faiblesses relatives à la sécurité. Introduction aux crypto-systèmes à clés privées et à clés publiques. Études des algorithmes existants (DES, RSA, etc.). Exemples de réalisation : KERBEROS, PGP, etc. Normes et architecture de sécurité de réseau. Gestion de clés. Gestion de transactions. Construction de «firewall». Aspects légaux.

- Systèmes de contrôle d'accès aux données (Informatique et Ingénierie, INF 6153)

Exigences de sécurité des données et de protection de la vie privée. Politiques de protection et contrôle d'accès d'entreprise. Méthodes de contrôle d'accès discrétionnaires et non-discrétionnaires, caractéristiques logiques et implémentation. Rôles d'entreprise. Conception de rôles. Contrôle d'accès basé sur les rôles (RBAC) et ses variantes. Contrôle d'accès basé sur les attributs. Méthodes Bell-LaPadula, Biba et muraille de Chine. Modèles hybrides. Langages pour la spécification d'exigences et de politiques de contrôle d'accès. Analyse de cohérence et complétude de politiques de contrôle d'accès. Principes et méthodes pour l'analyse du risque dans le contrôle d'accès. Étude de la littérature et d'outils courants.

- Cybercriminalité et techniques d'investigation (Informatique et Ingénierie, INF 1153)

Introduction à la cybercriminalité : accès non autorisé, altération de données, possession de cybermatériel prohibé (pornographie juvénile, etc.), possession d'outils de piratage. Aspects juridiques : système judiciaire canadien, lois sur la criminalité informatique, charte des droits et liberté, le droit commun. Processus d'investigation : planification de la recherche, déploiement de stratégies de collecte de données, reconnaissance de l'environnement, l'identification des éléments de preuve, construction et manipulation de preuves d'infractions dans le cyberespace, contamination de la preuve. Analyse de systèmes Microsoft. Analyse de systèmes Linux. Études de cas approfondies.

- Initiation à la sécurité informatique (Informatique et Ingénierie, INF 1433)

Concepts de base de la sécurité informatique. Menaces. Vulnérabilités des systèmes. Normes et analyse de risques. Survol des technologies utilisées en sécurité informatique : cryptographie, cryptanalyse, authentification, confidentialité, codes malicieux, pare-feux, audits, détection d'intrusions, etc. Vérification et maintenance d'un système d'information, sécurité des systèmes d'exploitation. Développement d'applications sécuritaires. Ce cours comporte des séances obligatoires de travaux dirigés (TD) de deux heures par semaine.

- Introduction à la cryptographie (Informatique et Ingénierie, INF 6163)

Introduction à la cryptographie: terminologie, fonctions cryptographiques ; exemples historiques de protocoles de cryptographie : la cryptographie classique, le chiffrement de Vigenère, le chiffrement de Hill; la cryptanalyse des crypto-systèmes classiques. La cryptographie moderne, protocoles de confidentialité : protocoles à clé secrète et à clé publique. Introduction aux fonctions booléennes; opérateurs logiques et polynômes. Cryptographie à clé secrète; diagrammes de Feistel ; D.E.S., la version simplifiée S-DES ; I.D.E.A.; S-IDEA. Le protocole A.E.S., S-AES: modes d'opération des chiffrements par blocs. Cryptanalyse des protocoles à clé secrète : confusion et diffusion ; cryptanalyse linéaire. Introduction à la théorie des nombres; les nombres premiers appliqués aux crypto-systèmes asymétriques. Concept de cryptographie à clé publique; algorithme RSA, gestion des clés, algorithme Diffie-Hellman; fonctions de hachage, algorithmes SHA-1et MD5; authentification des messages. Signatures numériques, standard DSS, authentification des protocoles.

Université Laval

- Sécurité, contrôle et gestion du risque (Systèmes d'information organisationnels, SIO 2102)

Les objectifs du cours sont de permettre à l'étudiant de comprendre et d'utiliser les principaux modèles de contrôle de la sécurité des systèmes d'information, de le rendre capable de repérer les forces et les faiblesses du système de sécurité d'une entreprise, de le rendre apte à développer une approche de gestion du risque et de la sécurité des systèmes d'information, ainsi qu'à proposer les correctifs nécessaires face à une situation risquée. Les techniques nécessaires aux affaires électroniques sont aussi considérées.

- Sécurité dans les réseaux informatiques (Informatique et génie logiciel, IFT 3201)

Concepts de base de la sécurité dans les réseaux informatiques. Les faiblesses des protocoles réseau. Les principales attaques réseau. Mise en place d'une politique de sécurité réseau. Propositions de stratégies de sécurité réseau : périmètre de sécurité, goulet d'étranglement, moindre privilège, confidentialité des flux réseau. Survol des technologies matérielles et logicielles. Protection des accès distants.

- Aspects pratiques de la sécurité informatique (Informatique et génie logiciel, IFT 2102)

Concepts de base de la sécurité informatique. Méthodologies, normes et analyse de risques. Survol des technologies : cryptographie, authentification, PKI, cartes à puces, etc. Architecture réseau, web, firewalls, audits, sécurité physique, détection d'intrusions, vérification et maintenance d'un système d'information. Développement d'applications sécuritaires. Identification des types d'outils et sources d'information.

- Informatique d'enquête (Informatique et génie logiciel, IFT 3002)

Origine d'une enquête informatique (computer forensics) et techniques d'enquête. Aspects informatique et judiciaire de la collecte et de l'analyse d'information, afin d'en assurer l'utilisation lors d'un procès. Localisation, extraction et divulgation des informations sur les systèmes d'exploitation, de stockage, les réseaux et les périphériques. Obstacle à l'enquête informatique. Étude de cas réels.

- Cryptographie and sécurité informatique (Informatique et génie logiciel, GLO 3100)

Systèmes cryptographiques symétriques (DES, AES, RC4, etc.), systèmes cryptographiques asymétriques (RSA, DSA, Elgamal, Courbes elliptiques, etc.), cryptanalyse, fonctions de hachage (MD5, SHA-1, etc.), protocoles cryptographiques (authentification, distribution de clés, etc.), applications (SSL/TLS, PGP, commerce électronique, etc.).

- Gestion de la sécurité des affaires électroniques (Systèmes d'information organisationnels, SIO 6005)

Les objectifs du cours sont de permettre à l'étudiant de comprendre et d'utiliser les principaux modèles de contrôle de la sécurité des affaires électroniques, de le rendre capable de repérer les forces et les faiblesses du système de sécurité d'une entreprise, de le rendre apte à développer une approche de gestion du risque et de la sécurité des affaires électroniques, ainsi qu'à proposer les correctifs nécessaires face à une situation risquée.

- Sécurité et méthodes formelles (Informatique et Ingénierie, INF 7010)

Ce cours vise l'étude de méthodes formelles modernes utilisées pour la spécification et la vérification de systèmes en général et des protocoles de sécurité en particulier. Nous démontrerons l'importance des protocoles cryptographiques, la subtilité de leur analyse et l'utilisation de méthodes formelles de spécification et de vérification (CCS/CSP, logique temporelle, « model-checking », etc.) comme solution incontournable pour assurer les objectifs de sécurité.

- Cryptologie et codage (Mathématiques et statistique, MAT 7310)

Rappels de théorie des nombres. Cryptosystèmes classiques. Algorithmes DES, AES, RSA. Logarithme discret. Signature digitale. Protocoles d'échanges de clés. Théorie de l'information. Courbes elliptiques. Codes correcteurs d'erreurs. Codes de Hamming, de Golay, BCH,RS.

Saskatchewan

University of Regina

- Cryptography and Network Security (Computer Science, CS 435)

Classical cryptosystems, data encryption standards, advanced encryption algorithms, public key cryptosystems, digital signatures, IP security, and web security.

- Risk and Reward in the Information Society (Computer Science, CS 280)

The history of computing and the social context of computing. Topics will include: methods and tools of analysis, professional and ethical responsibilities, risks and liabilities of computer-based systems, intellectual property, privacy and civil liberties, computer crime, and economic issues in computing.

University of Saskatchewan

- An Introduction to Information Security (Computer Science, CMPT 352.3)

Considers various aspects of security in information systems, both networked and non-networked. The challenges are managerial and administrative as well as technical. Students will have the opportunity to research real-world cases and to engage in classroom debates about current information security issues.