CSL COMPUTER NETWORK SECURITY GRADUATE PROGRAM OVERVIEW

References:

A. https://www.rmc-cmr.ca/en/registrars-office/graduate-programmes-electrical-engineering-and-computer-engineering
B. https://www.rmc-cmr.ca/en/registrars-office/master-public-administration
C. PG Computer Network Security, OSS AKQX, Approval Date - 30 July 2018
D. http://ece-rmc.ca/create/

Introduction

The RMC Computer Security Lab (CSL) offers graduate courses for both PhD and MASc programs of study. In addition to being accredited university programs outlined at references A and B, they also form foundational components of the Computer Network Security (CNS) Occupational Speciality Specification (OSS) at reference C and the *NSERC Cybersecurity CREATE* program outlined at reference D. Our program is centred around the courses in Table 1 below.

Table 1 – ECE Graduate AKQX Courses[1]

Course #	Course Title	Academic Year 20/21
EE502	Applied Research	Fall/Winter
EE547	Digital Forensics	Fall
EE569	Malware Analysis	Winter
EE578	Introduction to Computer Systems and Network Security[2]	Fall
EE580	Applied Cyber Operations	Winter
EE593	Advanced Traffic Analysis	Fall
EE595	Cyber Threat and Attack Techniques[3]	Fall
EE597	Operational Technology Cybersecurity[4]	Not offered in 20/21
MPA535	The Cyber Challenge	Spring/Summer
MPA591	Cyber Statecraft and National Security	Winter

Reference C states that officers will achieve the AKQX certification after completion of a formal course of study at the post-graduate level at the Royal Military College of Canada. Our CNS students may be:

a) Canadian Armed Forces (CAF) officers attending on PGT;
b) CAF Members studying CNS part-time; and
c) civilian students studying CNS.

[1] Note that MBA509 is a graduate cyber related course, however, a significant amount of the technical component of this course is covered in the existing ECE curriculum, it is not recommended for ECE MASc students.
[2] Students who graduated from the RMC BEng (Computer Engineering) since 2015 cannot take EE578 because of the wide amount of overlap with EEE/GEF330, EEE/GEF466 and EEE/GEF404.
[3] EE578 is a co-requisite to EE595.
[4] EE597 has a security clearance requirement.

Course descriptions for the courses in Table 1 may be found at reference A and at Annex A, which also includes course syllabi (for the ECE courses only).

PhD Program of Study

The typical program of study for CNS doctoral students is as follows, although a student may modify it with the concurrence of their respective supervisor(s):

- 4 Graduate Courses;
  - EE578 Computer Systems and Network Security
  - At least two other CNS course
    - Students who are not eligible to take EE578 are expected to take at least three other CNS courses
  - At most one elective graduate course from the RMC Electrical and Computer Engineering (ECE) Department, another RMC department or a civilian university
- Participation in at least two serials of CyberX;
- Comprehensive Exams; and
- A security related thesis.

MASc Program of Study

The typical program of study for CNS MASc students is as follows, although a student may modify it with the concurrence of their supervisor and as required, the ECE Graduate Studies Committee (ECE GSC):

- Six graduate courses;
  - EE502 Applied Research in Electrical and Computer Engineering
    - This course is required for all ECE Masters Students
  - EE578 Computer Systems and Network Security
  - At least two other CNS courses.
    - Students not eligible to take EE578 are expected to take at least three other CNS courses
  - At most two elective graduate courses from the RMC Electrical and Computer Engineering (ECE) Department, another RMC department or another university.
- Participation in at least two serials of CyberX; and
- A security related thesis.

Sponsored PGT Students

MASc students on sponsored Post-Graduate Training (PGT) normally chose a supervisor near the end of the Fall semester. Until a specific supervisor is agreed upon, all PGT students will fall under the supervision of the Software/Security member of the ECE GSC. All new PGT students will meet with Dr. Leblanc to construct a Program of Study during the week prior to the start of the graduate course calendar for the fall semester.

PGT students are encouraged to discuss potential areas of research with their sponsors, but they should not commit to researching a particular problem. Supervisors will be well positioned to help CNS graduate students define a problem that suits their interests and those of their sponsors.

The calendar descriptions and overview of each CNS course is listed below, in order of course number.

EE502 Applied Research

This course is normally taken by students in the Master of Applied Science Programme in Electrical, and Computer Engineering Department. The course provides an introduction to the primary and secondary sources of information in the literature of the associated disciplines. The students will also be exposed to the specific applied research groups within the Department, their techniques, and their specific application of the scientific method.

The students will conduct in-depth research in a specific topic area related to their field of study. A member of the Department Faculty will supervise this investigation through directed study. The Student will be required to communicate research ideas in writing though academic papers and proposals, and verbally through presentations and seminars. Standards for academic discourse and publication will be emphasized in the assigned papers and presentations.

Course Overview: The course consists of lectures, seminars and directed studies equivalent to a course of 3 periods per week for one term, spread across the fall and winter semesters. For students pursuing the Computer Network Security OSS the research topic for EE502 will typically be in the area of computer network security and will be supervised by a faculty member of the RMC CSL.

EE547 Digital Forensics

Digital forensics is a branch of forensic science which focuses on the recovery and analysis of information found in digital systems. It has a wide range of applications including intelligence gathering, private, corporate and criminal investigations, incident response involving digital systems and many others. In this course, students will develop a thorough understanding of digital forensics theory and techniques and will apply these to investigate incidents involving malicious user activity and malware on common operating systems. Topics will include image acquisition techniques, analysis of volatile and non-volatile memory, file systems structure, OS artifacts, e-mail systems, web browser activity, USB storage device activity, timeline of activity, data stream carving, deleted file carving, process analysis, network connection analysis and anti-forensic techniques.

Course Overview: Three contact hours per week for lecture and lab, this course also includes a course project. This is a single semester course.

Course Outline

Subjects	Topics
Principles of digital forensics	• Intro to digital forensics • Intro to incident response • Phases of a forensic investigation • Phases of an incident response operation • Key principles
Volumes and partitions	• Components of a hard drive • Volumes and partitions • Partitioning tables • Multi-disk volumes

Filesystems	• FAT
	• NTFS
	• Ext3
	• For each:
	  ○ History
	  ○ Concept of operation
	  ○ Deep Analysis of on-disk structures

Windows Forensics	• Windows Image Acquisition • Registry Analysis • Event Log Analysis • Evidence of File Download, Program Execution, File/Folder Opening, Deleted File or File Knowledge, Physical Location, External Device/USB, Account Usage, Browser Usage, Building a timeline, Summary of tools
Windows Memory Forensics	• Memory Management, Memory Acquisition • The Volatility Framework • Windows Executive Objects • Pool tag scanning • Analysing processes, handles, tokens • Analysing process internal memory • Hunting malware in process memory • Recovering event logs, registries • Networking artefacts • Kernel forensics and rootkits analysis

EE569 Malware Analysis

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 advanced topics in malware analysis.

Course Overview. Three contact hours per week for lecture and lab, this course also includes a seminar paper and final exam. This is a single semester course.

Course Outline

Topics
Basic Analysis: Basic Static Analysis Basic Dynamic Analysis
Advanced Static Analysis: x86 Assembly IDA Pro
Recognizing Code Constructs
Windows APIs and the Registry The Windows Boot Process Following Malware Execution
Advanced Dynamic Analysis: Debuggers OllyDbg Kernel Debugging
Malware Functionality: Malware Behaviour Malware Launching Data Encoding
Anti-reversing: Anti-reversing Techniques Packers & Unpacking
Seminar Presentations: Current research topics in malware analysis and reverse engineering

EE578 Computer Systems and Network Security

The course is meant as an introduction to the security issues associated with the security of computer systems and networks. The topics covered will include computer security concepts, terminology, seminal research, operating systems, and issues of network administration related to computer security, including the deployment and configuration of servers such as directory services. The course will discuss comprehensive aspects of security such as network attack, network zoning, segmentation and protection, intrusion techniques and the detection of such attacks and intrusions. Students undertake a series of lectures, assignments and laboratory exercises throughout the course.

Course Overview: Three contact hours per week for lecture and lab, this course also includes a course project. This is a single semester course.

Course Outline: <Under development>

EE580 Applied Cyber Operations

Cyber Operations are much more than the use of computers and networking technology; they require coordinated action to achieve a desired effect in cyberspace. This course will explore the application of cyber operations through the preparation for and participation in a major cyber exercise where students will design networks in support of a simulated military operation, build the network and operate it. Students will be required to operate in the face of a sophisticated and determined adversary with goals in direct opposition to the students, thereby generating simulated cyberspace conflict. In preparation for the simulated engagement, students will be required to build and deploy services such as directory, name resolution, electronic mail, web, file, etc. During the simulated engagement, students will be required to monitor these services, perform other network maintenance tasks, carry out intrusion detection and other simulated defensive cyber operations tasks, as well as participate in simulated offensive cyber operations. All students registered in the course will form part of a single team which will work cooperatively with teams of students from other academic programs against teams of adversaries composed of members from the military, government, and partner organizations.

Prerequisite: EE578 or similar experience in computer systems and network security

Course Overview: Lectures / Cyber Exercise: Equivalent to a course of 3 periods per week (one term)

Course Outline: <*Under development*>

.

EE593 Advanced Network Traffic Analysis

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.

Course Overview: Three periods per week for lecture and lab, this course also includes a seminar paper and course project. This is a single semester course.

Course Outline

Module 1	Traffic analysis refresher • Packets, flows, sessions, conversations • Review of signature detection and common analyst tools such as tcpdump, tshark and suricata. • Anomaly detection, Introduction to Zeek • Encrypted Communications

Module 2	Statistics refresher and introduction to data manipulation and visualization
	• Distributions
	• Confusion matrix, significance levels, entropy
	• Introduction to Natural Language Processing
	• Data plotting and visualization
	• Introduction to data science and visualization libraries and tools such as
	  ○ Sklearn
	  ○ Numpy
	  ○ Pandas
	  ○ NLTK
	  ○ Matplotlib, Seaborn, Plotly, Sandance for VSCode

Module 3	Introduction to machine learning
	• Linear algebra refresher
	• Supervised, unsupervised learning
	• Fundamentals such as:
	  ○ Hidden Markov Models
	  ○ K-Means and DBSCAN Clustering
	  ○ Principle Component Analysis (PCA)
	  ○ Support Vector Machines (SVMs)
	  ○ Data pre-processing, feature engineering and evaluating model performance

595 Cyber Threat and Attack Techniques

Those operating in the cyber domain 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, tunneling 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.

Course Overview: Three periods per week for lecture and lab, with a final exam. This is a single semester course.

Course Overview

Module	Topics
Overview	Threat Categories
	Risk Management
Linux Abuse	Unix Permissions - Interruptible Path
	Unix Permissions - SUID Issues
	Maintaining Access
Password Security	Password Cracking
	Pass the Hash
Web Exploits	Intro to SQL Injection
	Advanced SQL Injection
	Target Exploitation Frameworks
	Cross-Site Attacks
Binary Exploitation	Buffer Overflow Exploits
	Format String Attacks
	Remote Service Exploitation
	Return Oriented Programming
Penetration Testing	Metasploit and the Meterpreter Payload
	Pivoting
	Red Team Practical Exercise

EE597 Operational Technology (OT) Cybersecurity

Students will develop a thorough understanding of the components within operational technology (OT) and its similarities and differences with information technology (IT). The course will include offensive and defensive cybersecurity aspects of Operational Technologies at the application, network and physical layers. Components of the course will build on the foundations from civilian OT systems and protocols and focus on military platform security. There is a security clearance requirement for this course.

Course Overview: Three periods per week for lecture and lab, this course includes a seminar paper and course project. This is a single semester course.

Course Outline

Topics
Introduction • Terminology, context, differences/similarities between IT/OT), common SCADA protocols
OT Protocols • Understanding common OT protocols and their vulnerabilities such as MODBUS and DNP3. • CANBUS • MIL-STD-1553
OT Security Architecture • OT security architecture • VLAN security

OT Vulnerability Assessment
• Common methodologies and considerations
• Vulnerability Discovery
  ○ Smart Fuzzing
  ○ Guided Fuzzing

Hardware Security • Interfaces • Attack techniques and countermeasures

MPA535 The Cyber Challenge

This course will explore the digitized world (the good, the bad and the ugly) in the Canadian context with a view to assessing the breath and scope of the cyber reality within Canada and the policy challenges it poses, with emphasis on the Federal Government. Topics covered include cyberterrorism and cyberespionage, cybercrime, cyberwar, counterterrorism and the privacy/security conundrum. It will also discuss what Canada is/should/could be doing about the cyber threat and/or Internet Governance in the current legislative and constitutional context.

MPA591 Cyber Statecraft and National Security

The course introduces students to social science dimensions of offensive and defensive computer network operations, exploitation, attacks, and cyberwarfare. Its premise is cyber as a new domain of warfare that poses an existential threat to national security, prosperity and democracy. What difference does it make to think about democracy from the perspective of cyber - and about cyber from the perspective of democracy in general, and the Canadian democratic regime, its norms, values and underlying constitutional and governance principles in particular? The course's learning proposition is that cyber is not merely a technical but, fundamentally, a behavioural, policy, administrative, legal, economic, political, cultural, social and strategic challenge.