Computer Network Security Graduate Program

Ref: OSS AKQX – PG Computer Network Security, OSS AKQX, Approval Date: TBC 2018.

The RMC Computer Security Laboratory offers the following graduate courses, which we call Computer Networks Security (CNS) Courses:

- EE547 Forensics (Fall 2018)
- EE569 Malware Analysis (Winter 2019)
- EE579 Computer Systems and Network Security (Fall 2018 and Winter 2019)
    - The course spans the Fall and Winter semesters
    - Includes participation in CyberX for credit in the Winter of 2019
    - Students who graduated from the RMC BEng (Computer Engineering) since 2015 cannot take EE579 because of the wide amount of overlap with EEE/GEF330, EEE/GEF466 and EEE/GEF404.
- EE587 Topics in Computer Engineering – Operational Technologies (Winter 2019)
    - This course has a security clearance requirement
    - We expect the course number to change
- EE593 Advanced Network Traffic Analysis (Fall 2018)
- EE595 Cyber Threat and Attack Theory (Fall 2018)
    - EE579 is a co-requisite to EE595

The reference 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: 1) CAF officers attending on PGT, 2) CAF Members studying CNS part-time, and 3) civilian students studying CSN. The two graduate programs that usually lead to the certification are the Masters of Applied Science (MASc) and the doctorate (PhD).

CyberX

One of things that make our CNS graduate programs unique is participation in a major cyber exercise, which we call CyberX, where we ask students to *design* a network, *build* that network and *defend* that network in the face of attacks by a sophisticated adversary.

Our CNS graduate students and undergraduate computer engineering students each form a Blue Team and the Red Team attacking them is composed of members from outside units and agencies such as the US NSA, CFSCE, CFNOC, DIMEI, etc.

Participants in CyberX spend several weeks designing and building and integrating services for their networks during the winter semester, and they participate in Cyber Operations during the active phase of CyberX. The active phase of CyberX 2019 will take place from 8-11 April 2019.

We expect CNS graduate students to participate in CyberX at least twice during their program, whether they do so for credit as part of EE579 or as a general technical development activity.

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 the supervisor:

- 4 Graduate Courses
    - EE579 Computer Systems and Network Security.
    - At least two other CNS courses.
        - Students who are not eligible to take EE579 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
- 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 the supervisor:

- Six graduate courses
    - EE502 Applied Research in Electrical and Computer Engineering
        - This course is required for all ECE Masters Students
    - EE579 Computer Systems and Network Security.
    - At least two other CNS courses.
        - Students who are not eligible to take EE579 are expected to take at least three other CNS courses.
    - At most two 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
- A security related thesis.

Sponsored PGT Students

MASc students on sponsored PGT normally chose a supervisor near the end of the Fall semester. Dr. Leblanc provides advice in the meantime. All PGT students will meet with Dr. Leblanc to construct a Program of Study during the week of 4 - 7 September 2018.

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

The calendar descriptions and typical overviews of each CNS course follow, listed in increasing order by course number.

EE502 Applied Research (Fall 2018 on Wednesdays from 0800 – 1000hrs as needed, and Winter 2019)

This course is normally taken by students in the Master of Applied Science Programme in Electrical, Computer or Software Engineering. 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.

Lectures/Seminars/Directed Study (two terms):

Equivalent to a course of 3 periods per week for one term.

Course Overview:

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 (Fall 2018 on Wednesday from 1300 – 1600hrs)

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.

Lectures/Project: 3 periods per week plus laboratory plus project (one term)

Course Overview

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:
	  o History
	  o Concept of operation
	  o 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 (Winter 2019 at a time to be determined)

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.

Lectures:

3 periods per week plus laboratory plus project (one term)

Course Overview:

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 Memory-based Forensics
Seminar Presentations: Current research topics in malware analysis and reverse engineering

EE579 Computer Systems and Network Security (Fall 2018 on Monday from 1300 – 1600hrs and Winter 2019 as needed)

Topics will include computer security concepts, terminology, networking fundamentals, 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. Participation in a cyber defence exercise constitutes a major portion of this course.

Lectures/Cyber Exercise:

3 periods per week in the laboratory (8 weeks in the Fall term)
Preparation and participation in a cyber defence exercise (4 weeks in the Winter term)

Course Overview:

Subject	Topics
Networking & Packet Analysis	• Introduction to Networks • Link Layer Protocols
	• Network Layer Protocols • Transport Layer Protocols • VLANs
	• Introduction to Traffic Analysis • Man-in-the-Middle attacks
Network Defence	• Intrusion Detection Systems • Survey of Attack Techniques
	• Reconnaissance Scanning • Vulnerability Assessment
	• Zone Security (ITSG-32) • Firewalls
Host / Server Defence	• Symmetric and Asymmetric Cryptography • Passwords and Access Control • Operating System Security
	• Common Network Services (DNS, Web, Mail, AD, ...) • Server Hardening

CyberX

Preparation for and participation in CyberX is an integral part of the course. This will include research into an assigned task or service (the task assignments will be done in October), the building of servers and workstations and participation in the active phase of CyberX. All told, course deliverables associated to CyberX will account for more than 2/3 of a student's EE579 mark.

EE587 Operational Technology Cybersecurity (Winter 2019 at a time to be determined)

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.

Lectures:

3 periods per week plus laboratory and project (one term)

Topics
Introduction • Terminology, context, differences/similarities between IT/OT), common SCADA protocols
OT Network Protocols • Understanding common OT protocols and their vulnerabilities such as MODBUS and DNP3. • Protocol analysis lab
OT Security Architecture • OT security architecture considerations and potential solutions • VLAN security lab
OT Vulnerability Assessment • Common methodologies and considerations • Fuzzing lab
Hardware Security • Common interfaces, attack types (e.g. side-channel attacks) • Hardware security lab
Academic paper review and presentation on OT security
Course Project

EE593 Advanced Network Traffic Analysis (Fall 2018 on Tuesday from 0900 – 1200hrs)

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.

Lectures/Project:

3 periods per week plus laboratory plus project (one term)

Course Overview:

Topics
Basic Statistics Probability distribution functions Hypothesis testing
Network Traffic Measurements (Features) Packets, flows, connections, conversations Basic Statistics (size-based, time-based) Entropy N-grams
Traffic Characterization Traffic characterization techniques & tools Traffic type mental modeling
Anomaly Detection Statistical techniques Machine learning techniques Data mining techniques
Traffic Classification Supervised vs unsupervised Survey of techniques Feature selection algorithms
Evaluating Experimental Results Review sensitivity vs specificity ROC curves Cross-validation
Seminar Topics: Current research topics in intrusion detection and machine learning

EE595 Cyber Threat and Attack Techniques (Fall 2018 on Tuesday from 1300 – 1430hrs and Thursday from 0900 – 1050hrs)

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.

Lectures/Seminars/Project:

3 periods per week plus laboratory plus project (one term)

Course Overview:

Topics
Threat Categories Risk Management Unix Permissions - Interruptible Path
Unix Permissions - SUID Issues
Maintaining root Access
Privilege Escalation - Password Cracking
Pass the Hash
Intro to SQL Injection
Advanced SQL Injection
Target Exploitation Framework
The Meterpreter Payload
Pivoting
Buffer Overflow Exploits
Format String Attacks
Return Oriented Programming
Fuzzing