GEORGIAN COLLEGE

COMPUTER AND NETWORK SYSTEMS SECURITY

Program Outline

Major: CNSS
Length: 1 Year
Delivery: 3 Semesters
Credential: Ontario College Graduate Certificate
Effective: 2014-2015
Location: Barrie
Start: Fall (Barrie)

Description

The Computer and Network Systems Security post graduate program prepares students for careers involving the development, evaluation, and support of IT security solutions. Building on previous educational experience, students learn to create cost effective and secure computing environments. Graduates are able to categorize, design, implement, and integrate technical and managerial safeguards to ensure the security of networked computer systems. As well, graduates acquire the skills to formulate, propose, and organize security policies and procedures to protect corporate information assets including legal, regulatory and governance issues.

Career Opportunities

The need for organizations to generate secure network and information systems has created demand for skilled computer and network systems security specialists. Chief Information Officers and Information Technology Managers charged with the need to plan and implement security controls and infrastructure to protect corporate information systems will increasingly require the skills of security specialists. Career opportunities will be available in both public and private sector organizations. Graduates will gain employment as network and systems administrators or technicians.

Program Learning Outcomes

The graduate has reliably demonstrated the ability to:

- collect, analyze and review information for the identification of essential data and systems including possible threats, damage and loss;
- establish organizational policies for proper use and protection of information assets including contingency and disaster plans for backup, recovery and/or replacement of systems and data;
- review legal, ethical, regulatory and corporate governance issues;
- implement and configure networking hardware devices such as servers, routers, and switches as well as wireless devices for optimum security;
- deploy and manage desktop and server operating systems and optimize system settings in order to 'harden' information systems;
- install specific hardware and applications software for secure transmission in web and e-commerce systems including but not limited to access control, authentication, and encryption;
- select and apply prevention techniques and countermeasures for dealing with malicious threats to information such as viruses, worms and Trojan horses;
- install and configure network monitoring and security management utilities for the identification and measurement of possible system attacks or misuse;
- manage network operations including policies, standards and procedures to define users in terms of what they can do, resources they can access, and operations they are allowed to perform;
- apply and use network and operating system utilities with an emphasis on deploying preventative measures and procedures;
- formulate and implement a migration plan that allows for the safe upgrading of networks, operating systems, and/or application software while maintaining stability and security;
- acquire the knowledge and hands-on skills needed to prepare for industry-recognized information security certification exams.

The Program Progression:

```
Fall Intake - Barrie

Sem 1 | Sem 2  | Sem 3
----------------------
Fall  | Winter | Summer
2014  | 2015   | 2015
```

Admission Requirements:

Applicants must meet ONE of the following requirements to be eligible for admission to this program:
- College diploma or university degree with a focus in computer studies, or equivalent work experience in computer networks and operating systems.

Selection Process:
Applicants will be asked to submit a current resume and letter of interest to the Program Coordinator. Academic and experiential learning of all applicants will be assessed.

Criminal Reference Check:
Placement agencies require an up-to-date clear criminal reference check and vulnerable sector check prior to going out on placement. Students should obtain their criminal reference check approximately one month prior to placement; checks conducted earlier may not be considered current. As some jurisdictions require longer lead-time for processing, please check with the program co-ordinator to ensure you allow for sufficient turn-around time. Students are required to provide these checks prior to placement start.

NOTE: A record of criminal offences, for which a pardon has not been granted, may prevent the student from completing their placement, thereby affecting their ability to graduate.

Additional Information:
To be successful in this program, you are required to have a personal notebook computer (either PC or Mac architecture) prior to the start of the program that meets or exceeds the following hardware specifications:
- Intel I3 processor or AMD equivalent
- 4GB of memory
- 250GB hard drive

Additional operating systems, security tools, and software used in the program will be provided to the student upon commencement of the program.

Graduation Requirements:
12 Mandatory Courses
1 Internship

Graduation Eligibility:
To graduate from this program, a student must attain a minimum of 60% or a letter

grade of P (Pass) or S (Satisfactory) in each course in each semester. The passing weighted average for promotion through each semester and to graduate is 60%.

Mandatory Courses
NETS1006 Contingency Planning and Disaster Recovery
NETS1015 Security Management
NETS1016 Security Trends and Issues
NETS1024 Computer Security
NETS1025 Network Security 1
NETS1026 Windows Systems Security
NETS1027 Secure Network Architecture
NETS1028 Linux Systems Security
NETS1029 Securing Wireless Networks
NETS1030 Networks Security 2
NETS1031 Cyberspace Security
NETS1032 Auditing and Forensics

Internship
NETS1033 Computer and Network Systems Security Internship

Course Descriptions:
NETS1006 Contingency Planning and Disaster Recovery 42.0 Hours
This course examines the methods and techniques used to safeguard organizations from serious threats to the normal continuation of business activities due to disastrous events and unplanned disruption to essential services. Students will learn the difference and relationship between Business Recovery Planning and Disaster Recovery Planning, and how to apply the principles of each. Emphasis will be placed upon the practical application of vulnerability and risk assessment, planning, strategies for recovery and implementation of plans and policies.

NETS1015 Security Management 42.0 Hours
This course emphasizes the development and promotion of an information security mission for an organization in accordance with its overall goals and objectives. Students will learn how to identify the roles and responsibilities of each member of an organization in order to develop controls that provide security while maintaining adequate access. Issues such as employment practices, procedures and agreements will be discussed along with policy formation, security awareness training and data classification.

NETS1016 Security Trends and Issues 42.0 Hours
In this course, students examine the most current trends and issues related to computer, network, web, mobile, and ubiquitous computing security. Students research

and discuss IT security topics such as major security breaches from resources such as the web, trade publications, association newsletters, and the popular media.

NETS1024 Computer Security 42.0 Hours
This course examines how to limit access to workstations, servers, and mobile systems. Students will learn various techniques of system hardening, applying rights and permission, and penetration testing. Common types of computer attacks are also studied, along with prevention methods.

NETS1025 Network Security 1 42.0 Hours
Students learn that controlling network information access is critical to information systems security. Various types and techniques of network access control, rights and permissions are studied, as well as local network and remote access authentication and identification techniques. This course also examines the equipment, methods, and protocols used for the transmission and protection of information. Other topics studied include email and web security, attacks and countermeasures, fraud and abuse.

NETS1026 Windows Systems Security 42.0 Hours
In this course, students learn to apply security industry best practices and to harden the Windows operating system in a variety of configurations and roles. Students learn how to protect Windows-based systems from attacks, reconfigure the operating system to fully protect it, and scan hosts for known security problems. By the end of the course, students have a solid understanding of the security architectures used by Windows operating systems.

NETS1027 Secure Network Architecture 42.0 Hours
This course examines the concepts and techniques for designing and implementing reliable, secure, and manageable networked systems. Students learn to analyze business and technical requirements, examine traffic flow and Quality of Service (QoS) requirements, and select protocols and technologies based on performance and security goals. Integrated design is examined for the secure interoperation of wireless, Virtual Private Networks (VPN), Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), Voice over IP (VolP), redundancy, and Ethernet scalability.

NETS1028 Linux Systems Security 42.0 Hours
In this course, students learn how to secure all major aspects of Linux/Unix operating systems, balancing security issues with the purpose of the system and the needs of an organization. Students learn how to tune kernel and operating system parameters, deactivate components, and tighten the components that remain.

NETS1029 Securing Wireless Networks 42.0 Hours
In this course, students gain the knowledge and skills to defend against intrusion within wireless networks. Students learn to detect weaknesses in existing networks, design and configure effective security solutions, secure wireless networks against threats and

attacks, analyze and react to wireless denial-of-service (DOS) attacks, use encryption to provide privacy and authenticity, and implement the latest wireless security standards to protect wireless data networks.

NETS1030 Networks Security 2 42.0 Hours
The Network Security 2 course focuses on the overall security of a network. It expands on the knowledge gained in Network Security 1 and introduces the concepts of Intrusion Prevention (IPS) and Virtual Private Networks (VPNs). Topics include security technologies, products and solutions; firewall and secure router design, installation and configuration; intrusion prevention implementation using routers; and VPN implementation using routers; and firewalls.
P- NETS1025 Network Security 1

NETS1031 Cyberspace Security 42.0 Hours
Students examine the economic foundations of electronic commerce and the main technologies used to implement online business activities. Electronic commerce software, payment systems, purchasing, data interchange, supply-chain management, auction sites, virtual communities and their respective security threats and countermeasures are examined. Legal, ethical, and regulatory internet issues are also studied.

NETS1032 Auditing and Forensics 42.0 Hours
In this course, students apply the principles of computer forensics in order to detect, track and prevent network intrusions. Students will learn how to collect analyze and interpret data collected from various sources. as well as examine different methods of recovering and examining digital evidence.

NETS1033 Computer and Network Systems Security Internship 560.0 Hours
The Internship component of the Computer and Network Systems Security program involves a process by which students integrate their academic education with work experience related to their program of study. This integration reinforces skills and theory learned during academic semesters, develops professional contacts, job knowledge and career paths, improves human relations and communications skills and promotes personal maturity and financial independence.
P- NETS1006 Contingency Planning and Disaster Recovery and P- NETS1015 Security Management and P- NETS1026 Windows Systems Security and P- NETS1028 Linux Systems Security and P- NETS1029 Securing Wireless Networks and P- NETS1030 Networks Security 2 and P- NETS1031 Cyberspace Security and P- NETS1032 Auditing and Forensics

Course Description Legend
P = Prerequisite; C = Concurrent prerequisite; CO= Corequisite

Information contained in College documents respecting programs is correct at the time of publication. Academic content of programs and courses is revised on an ongoing basis to ensure relevance to changing educational objectives and employment market needs. The college reserves the right to add or delete programs, options, courses, timetables or campus locations subject to sufficient enrolment, and the availability of courses.