Course Outline

School:	Eng. Tech. & Applied Science
Department:	Information and Communication Engineering Technology (ICET)
Course Title:	Software Security
Course Code:	COMP 307
Course Hours/Credits:	56
Prerequisites:	COMP 212, COMP 228
Co-requisites:	N/A
Eligible for Prior Learning, Assessment and Recognition:	Yes
Originated by:	Joanne Filotti
Creation Date:	Summer 2013
Revised by:	Arben Tapia
Revision Date:	Summer 2014
Current Semester:	Fall 2018
Approved by:	ppesikan c/o

Chairperson/Dean

Students are expected to review and understand all areas of the course outline.

Retain this course outline for future transfer credit applications. A fee may be charged for additional copies.

This course outline is available in alternative formats upon request.

Acknowledgement of Traditional Lands

Centennial is proud to be a part of a rich history of education in this province and in this city. We acknowledge that we are on the treaty lands and territory of the Mississaugas of the Credit First Nation and pay tribute to their legacy and the legacy of all First Peoples of Canada, as we strengthen ties with the communities we serve and build the future through learning and through our graduates. Today the traditional meeting place of Toronto is still home to many Indigenous People from across Turtle Island and we are grateful to have the opportunity to work in the communities that have grown in the treaty lands of the Mississaugas. We acknowledge that we are all treaty people and accept our responsibility to honor all our relations.

Course Description

Students enrolled in Software Security will learn how to build secure software by becoming familiar with current software security principles. Students will also examine common application security flaws, and understand how to integrate security with design, development, testing and deployment phases of the software development life cycle. COMP307 addresses the ever-growing security concerns that IT organizations face regarding their deployed software applications. Students will also learn how to implement security strategies currently used to mitigate the security risks associated with web applications and social networking.

Program Outcomes

Successful completion of this and other courses in the program culminates in the achievement of the Vocational Learning Outcomes (program outcomes) set by the Ministry of Advanced Education and Skills Development in the Program Standard. The VLOs express the learning a student must reliably demonstrate before graduation. To ensure a meaningful learning experience and to better understand how this course and program prepare graduates for success, students are encouraged to review the Program Standard by visiting http://www.tcu.gov.on.ca/pepg/audiences/colleges/progstan/. For apprenticeship-based programs, visit http://www.collegeoftrades.ca/training-standards.

Course Learning Outcomes

The student will reliably demonstrate the ability to:

1. Understand and apply secure software design principles
2. Compare and Contrast the Secure Software Development Life Cycle (SSDLC) with the usual SDLC.
3. Apply Security Principles to implement User Authentication and Authorization (UA&A).
4. Implement Correct User and Session Management.
5. Apply proper Data Validation techniques to prevent intrusion attacks.
6. Implement client-side security.
7. Use error-handling and exception management correctly.
8. Apply auditing and logging to enhance security.

Essential Employability Skills (EES)

The student will reliably demonstrate the ability to*:

1. Communicate clearly, concisely and correctly in the written, spoken, and visual form that fulfills the purpose and meets the needs of the audience.
2. Respond to written, spoken, or visual messages in a manner that ensures effective communication.
4. Apply a systematic approach to solve problems.
5. Use a variety of thinking skills to anticipate and solve problems.
6. Locate, select, organize, and document information using appropriate technology and information systems.
7. Analyze, evaluate, and apply relevant information from a variety of sources.
8. Show respect for diverse opinions, values belief systems, and contributions of others.
9. Interact with others in groups or teams in ways that contribute to effective working relationships and the achievement of goals.
10. Manage the use of time and other resources to complete projects.

**There are 11 Essential Employability Skills outcomes as per the Ministry Program Standard. Of these 11 outcomes, the following will be assessed in this course.*

Global Citizenship and Equity (GC&E) Outcomes

The student will reliably demonstrate the ability to*:

1. Identify one's roles and responsibilities as a global citizen in personal and professional life.
4. Analyze the use of the world's resources to achieve sustainability and equitable distribution at the personal, professional, and global level.
5. Identify and challenge unjust practices in local and global systems.

**There are 6 institutional Global Citizenship & Equity outcomes. Of these 6 outcomes, the following will be assessed in this course.*

Text and other Instructional/Learning Materials

Text Book(s):

Harwood, M. 2011. Security Strategies in Web applications and Social Networking. Jones & Bartlett Learning.

ISBN 13: 978 0763791957

Online Resource(s):

Additional online materials will be used during lectures and labs.

Material(s) required for completing this course:

Additional hand-outs and/or online materials will be used during lectures and labs.

Evaluation Scheme

- Assignments, labs: Assignments, labs
- In-class discussions: This includes in-class work that will lead to discussions in groups.
- Test #1: Test for the material of Weeks#1-#5
- Test #2: Test for the material of Weeks#6-#10
- Last Test: Test for Weeks #1-#10 (20% of mark) and Week#11- Week#14 (80% of mark)

Evaluation Name	CLO(s)	EES Outcome(s)	GCE Outcome(s)	Weight/100
Assignments, labs	1, 2, 3, 4, 5	1, 2, 4, 5, 6		20
In-class discussions	1, 2	1, 2, 5, 6, 8, 9	1, 4, 5	15
Test #1	1	1, 2, 4, 5, 7		20
Test #2	2, 3, 4, 5, 6	1, 2, 4	1	20
Last Test	1, 2, 7, 8	1, 2, 6, 7, 10		25
Total				100%

If students are unable to write a test they should immediately contact their professor or program Chair for advice. In exceptional and well documented circumstances (e.g. unforeseen family problems, serious illness, or death of a close family member), students may be able to write a make-up test.

All submitted work may be reviewed for authenticity and originality utilizing Turnitin®. Students who do not wish to have their work submitted to Turnitin® must, by the end of the second week of class, communicate this in writing to the instructor and make mutually agreeable alternate arrangements.

When writing tests, students must be able to produce official College photo identification or they may be refused the right to take the test or test results will be void.

Student Accommodation

Students with permanent or temporary accommodations who require academic accommodations are encouraged to register with the Centre for Students with Disabilities (CSD) located at Ashtonbee (L1-04), Progress (C1-03), Morningside (Rm 190), and Story Arts Campus (Rm 284). Documentation outlining the functional limitations of a disability is required; however, interim accommodations pending receipt of documentation may be possible. This service is free and confidential. For more information, please email csd@centennialcollege.ca.

Use of Dictionaries

- Dictionaries may be used in tests and examinations, or in portions of tests and examinations, as long as they are non-electronic (not capable of storing information) and hard copy (reviewed by the invigilator to ensure notes are not incorporated that would affect test or examination integrity).

Program or School Policies

N/A

Course Policies

N/A

College Policies

Students should familiarize themselves with all College Policies that cover academic matters and student conduct.

All students and employees have the right to study and work in an environment that is free from

discrimination and harassment and promotes respect and equity. Centennial policies ensure all incidents of harassment, discrimination, bullying and violence will be addressed and responded to accordingly.

Academic honesty is integral to the learning process and a necessary ingredient of academic integrity. Academic dishonesty includes cheating, plagiarism, and impersonation. All of these occur when the work of others is presented by a student as their own and/or without citing sources of information. Breaches of academic honesty may result in a failing grade on the assignment/course, suspension or expulsion from the college.

For more information on these and other policies, please visit www.centennialcollege.ca/about-centennial/college-overview/college-policies.

Students enrolled in a joint or collaborative program are subject to the partner institution's academic policies.

PLAR Process

This course is eligible for Prior Learning Assessment and Recognition (PLAR). PLAR is a process by which course credit may be granted for past learning acquired through work or other life experiences. The PLAR process involves completing an assessment (portfolio, test, assignment, etc.) that reliably demonstrates achievement of the course learning outcomes. Contact the academic school to obtain information on the PLAR process and the required assessment.

Semester:	Fall 2018	Professor Name:	Bindu Goel
Section Code:	004-005	Contact Information:	email: bgoel@my.centennialcollege.ca phone 3587 Room No A-230
Meeting Time & Location:	Sec004: Tues 12.30-2.20 A3-13 Lab Tues 2.30-4.20 A1-61 Lecture Sec 005 Mon 8.30-10.20 A3-11 Lab Wed 12.30-2.20 A3-15 lecture	Office Hours:	Tue 12-12.30 or by apptmt

Topical Outline (subject to change):

Week	Topics	Readings/Materials	Weekly Learning Outcome(s)	Instructional Strategies	Evaluation Name	Evaluation Date
01	Introduction to Application Security . Evolution of data processing . Key areas of concern for ecommerce security . Lack of security in protocols . Securing communications	Chapter 1 Additional online reading materials	Ability to: - identify highlights in the evolution of data processing, from mainframes to the World Wide Web (WWW) - identify challenges involved in implementing security	- lectures - demonstrations - hands-on exercises - class discussions		
02	Impact of the Internet on Business . Challenges associated with the shift from traditional to online business models . E-business problem-solving and strategies . Changes in the risk landscape as business moves online	Chapter 2 Additional online reading materials	- analyze the impact of the Internet and Web applications on the business world	- lectures - demonstrations - hands-on exercises - class discussions	Assignment (Consequences of compromised security for Web apps)	

Week	Topics	Readings/Materials	Weekly Learning Outcome(s)	Instructional Strategies	Evaluation Name	Evaluation Date
03,04	Secure Communication . Key technologies in social media and social networking . Different types of online personal and business communications . Types of online attacks and perpetrators . Security and privacy risks related to use of social media and social networking	Chapters 3, 4 Additional online reading materials	Ability to: - analyze the evolution of people-to-people communications - analyze online personal and business communications and the threats to those communications	- lectures - demonstrations - hands-on exercises - class discussions	In-class assignment (Personal info exposed on the Internet)	
05,06	Mitigating Risks When Connecting to the Internet . Web site risks, threats, and vulnerabilities . Approaches to Web hosting . Best practices while connecting to the Internet . Test #1 Review . Test #1	Chapter 5 Additional online reading materials	Ability to: - Describe best practices for connecting to the Internet and securing a network perimeter	- lectures - demonstrations - hands-on exercises - class discussions - Test Review	Test #1 (20% of Final Mark)	
07,08	Mitigating Web Site Risks, Threats, and Vulnerabilities . Common vulnerabilities and attacks impacting Web applications . Best practices for mitigating known Web application risks, threats, and vulnerabilities	Chapters 6, 7 Additional online reading materials	- compare and contrast Web based risks - analyze common Web site attacks, weaknesses, and security best practices	- lectures - demonstrations - hands-on exercises - class discussions	In-class assignment (OWASP resources)	

Week	Topics	Readings/Materials	Weekly Learning Outcome(s)	Instructional Strategies	Evaluation Name	Evaluation Date
	. WASC Threat Classification					
09	Securing Web Applications . Technologies and systems used to make a complete functional Web site . Secure software development life cycle (SDLC) approaches . Best practices in securing Web applications	Chapters 8, 9	Ability to: - describe the attributes and qualities of the software development life cycle (SDLC)	- demonstrations - hands-on exercises - class discussions	In-class Assignment (Best practices for securing Web apps)	
10	E-Commerce Security . Audit and compliance obligations . Consequences for noncompliance . Payment Card Security . Public and private sector regulations . Configuration and change management, QA testing . Monitoring production applications . Strategies and best practices . Review for Test#2 . Test #2 (for Week#6-Week#10)	Chapters 10, 11 Additional online reading materials	Ability to: - analyze the role and importance of audit and compliance to Web application security - analyze the role and importance of quality assurance (QA) testing for Web applications	- lectures - demonstrations - hands-on exercises - class discussions	Test #2 - 20% of final mark.	
11	Performing Vulnerability and Security Assessments . Difference between	Chapter 12 Additional online reading materials	Ability to: - explain the value and importance of vulnerability and security assessments for Web applications	- lectures - demonstrations - hands-on exercises - class discussions	LabAssignment (Web app security assessment)	

Week	Topics	Readings/Materials	Weekly Learning Outcome(s)	Instructional Strategies	Evaluation Name	Evaluation Date
	audit, testing, and assessment . Main steps in security assessments . Techniques and best practices in security assessments					
12	Mobile Applications Security . Mobile computing . Authentication technologies . Overall impact on the risk landscape . Store-and-forward communications . Real-time communications . Best practices	Chapters 13, 14 Additional online reading materials	Ability to: - describe popular endpoint communications devices and their security risks - store-and-forward and real-time communications, and the threats against them	- lectures - demonstrations - hands-on exercises - class discussions		
13	Special Security Topics . Security organizations . Security education and training . Security certifications . Qualifications applicable to students' areas of interest REVIEW	Chapter 15 Additional online reading materials	Ability to: - explain the responsibilities and interests of various national and international security organizations	- lectures - demonstrations - hands-on exercises - class discussions REVIEW		
14	Last Test	Last Test Review	Final Test . Week#1-#10 (20% of mark) . Week#11-#14 (80% of mark) Total Mark - 25% of Final Mark	Last Test	Last Test	