UVic Department of Electrical and Computer Engineering

COURSE OUTLINE
SENG 460 – Practice of Information Security and Privacy
Spring 2014

Instructor:

Dr. Henry Lee
Phone:
E-mail: henrylee@ece.uvic.ca

Office Hours:

Days: Fridays
Time: 11:00am – noon
Location: EOW419

Lectures:

A-sections: A01 / CRN 22713 A02 / CRN 22714
Days: Fridays
Time: 1:30pm – 4:20pm
Location: Clearihue (CLE) Building A202

Optional Text:

Title: Practice of Information Security
Author: Henry Lee *et al.*, Province of British Columbia
Available at the Bookstore
Year: Winter 2013

References:

References and recommended further reading are provided in the text in every chapter. Lecture material for each topic will be available after each lecture at http://www.ece.uvic.ca/~henrylee/currentcourse.html.

Assessment:

Assignments:	30%	
Mid-term	20%	Date: Friday, Feb. 21st (1:30 – 3:30 p.m.)
Final	50%	Date: April (TBD)

Note: To complete the course, it is required to successfully complete all assignments. Each lecture contains a case study chosen from examples in the field. In the case study, a problem is described and students are asked to create solutions to the problem either cooperatively or individually. The result of the case study should be summarized individually and submitted to Dr. Lee as an assignment. *It is encouraged to develop the case study further and incorporate further findings into the assignment*.

Due dates for assignments:

Assignments will be due one week after they are assigned. All assignment deliverables must be submitted to Dr. Lee's ECE Dept. mailbox in EOW 448 by 4:30 p.m. on the due date (following Friday after each lecture). A 1% deduction in the overall assignment mark will be made for each day a given deliverable is late. After the submission timeline, the late assignment must be submitted via email to Dr. Lee at henrylee@ece.uvic.ca to verify the timestamp of the submission.

The final grade obtained from the above marking scheme will be based on the following percentage-to-grade point conversion:

Passing Grades	**Grade Point Value**	**Percentage for Instructor Use Only**	
A+ A A-	9 8 7	90-100 85-89 80-84	
B+ B B-	6 5 4	77-79 73-76 70-72	
C+ C	3 2	65-69 60-64	
D	1	50-59	
Failing Grades	**Grade Point Value**	**Percentage for Instructor Use Only**	**Description**
E	0	35-49	Fail, conditional supplemental exam. (For undergraduate courses only)
F	0	0-49	Fail, no supplemental exam.
N	0	0-49	Did not write examination, Lab or otherwise complete course requirements by the end of the term or session; no supplemental exam.

The rules for supplemental examinations are found on pages 80 of the current 2013/14 Undergraduate Calendar.

Term in which E Grade was obtained:	**Application Deadline for Supplemental Exam**	**Supplemental Exam Date**
First term of Winter Session (Sept – Dec)	February 28 in the following term	First week of following May
Second term of Winter Session (Jan – Apr)	June 30 in the following term	First week of following September
Summer Session (May – Aug)	October 31 in the following term	First week of following January

Deferred exams will normally be written at the start of the student's next academic term; i.e., approximately 4 months following the deferral of the exam.

Course Description

1. Course Objectives

This course is designed to address important issues to implement security in the corporate environment and deals with advanced topics in information security management. The course is aimed to provide practical understanding of information security based on the theory and practice. It is assumed that students have fundamental knowledge of information security. The course consists of 11 topics in information security and is delivered by 11 security practitioners from industry and government.

2. Learning Outcomes

Students will learn the foundational knowledge of the information security domains that are commonly classified by major information security personnel’s associations. It will bring a comprehensive view of information security and students will be familiar with the corporate information security requirements and problem solving approaches.

3. Syllabus

Enterprise Security Architecture. Information Security Policy and International Standards. Security Threat and Risk Assessment. Logging and Monitoring. Investigations. Application Security. Ethical Hacking. Privacy. Business Continuity Management. Physical and Environmental Security. Information Security as a Career.

Note to Students:

Students who have issues with the conduct of the course should discuss them with the instructor first. If these discussions do not resolve the issue, then students should feel free to contact the ECE Chair by email or the ECE Chair's secretary to set up an appointment.

Accommodation of Religious Observance

See http://web.uvic.ca/calendar2013/GI/GUPo.html

Policy on Inclusivity and Diversity

See http://web.uvic.ca/calendar2013/GI/GUPo.html

Standards of Professional Behaviour

You are advised to read the Faculty of Engineering document Standards for Professional Behaviour at http://www.uvic.ca/engineering/current/undergrad/index.php#section0-25 which contains important information regarding conduct in courses, labs, and in the general use of facilities.

Cheating, plagiarism and other forms of academic fraud are taken very seriously by both the University and the Department. You should consult http://web.uvic.ca/calendar2013/FACS/UnIn/UARe/PoAcI.html for the UVic policy on academic integrity.

Plagiarism detection software may be used to aid the instructor and/or TA's in the review and grading of some or all of the work you submit.