Western University
Faculty of Engineering
Department of Electrical and Computer Engineering

SE 4472a: Information Security

Course Outline - Fall 2018

Description: This course provides an introduction to the topic of information security in the context of network communication. It is intended for students who have some understanding of networks, but not necessarily any background in security. The goal of the course is to provide students with a foundation that will help them to identify, analyze and make appropriate security decisions during the design and deployment of information and network systems.

The course will cover selected security topics in the following areas:

- **Cryptography:** Formal notions of security. Classical cryptosystems, symmetric key encryption, public key encryption, digital signatures, hash functions, message authentication codes, true- and pseudo-random number generation, entropy and key length selection.
- **Access Control:** Authentication and authorization, digital certificates (certificate chains, trust stores), secure password generation and storage.
- **Protocols:** SSL/TLS connections (handshake, cipher suites agreement, establishing session keys), SSH. Public key infrastructure issues (issuing, checking and revoking certificates).

Instructor: Dr. Aleksander Essex
Office: TEB 235. Phone: (519) 661-2111 ext 87290. Email: aessex@uwo.ca
Course website: whisperlab.org/security
Consultation/office hour: TBD.

Academic Calendar Copy:

http://www.westerncalendar.uwo.ca/Courses.cfm?CourseAcadCalendarID=MAIN_017915_1&SelectedCalendar=Live&ArchiveID=

Contact Hours: 3 lecture hours, 2 tutorial hours, 0.5 course.

Prerequisites (for SE4472 only): ECE 4436A/B or Computer Science 3357A/B, SE 3313A/B or Computer Science 3305A/B.

Unless you have either the requisites for this course or written special permission from your Dean to enroll in it, you will be removed from this course and it will be deleted from your record. This decision may not be appealed. You will receive no adjustment to your fees in the event that you are dropped from a course for failing to have the necessary prerequisites.

CEAB Academic Units: Engineering Science 75%, Engineering Design 25%.

Required Textbook:

William Stallings. **Cryptography and Network Security: Principles and Practice**, 6/E, Pearson Higher Education, 2014. ISBN-10: 0133354695.

Other Required References:

- E. Rescorla. **The Transport Layer Security (TLS) Protocol Version 1.3.** RFC 8446. Available online: https://tools.ietf.org/html/rfc8446
- T. Dierks and E. Rescorla. **The Transport Layer Security (TLS) Protocol Version 1.2.** RFC 5346. Available online: https://tools.ietf.org/html/rfc5246
- Elaine Barker and Allen Roginsky. **Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths.** NIST Special Publication 800-131A Revision 1, 2015. Available online: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf

Recommended References:

- Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. **Handbook of Applied Cryptography**. CRC Press, 2001.
  Available online: http://cacr.uwaterloo.ca/hac/
- Nigel Smart. **Cryptography, an Introduction**. Online textbook, 2013.
  Available online: https://www.cs.bris.ac.uk/~nigel/Crypto_Book/

General Learning Objectives (CEAB Graduate Attributes)

Knowledge Base	3/2	Use of Engineering Tools		Impact on Society and the Environment	2/2
Problem Analysis	2/2	Individual and Team Work		Ethics and Equity	
Investigation	3/2	Communication Skills		Economics and Project Management	
Design	2/3	Professionalism	1/1	Life-Long Learning	

Notation: *x*/*y*, where *x* is the cognitive level (1: Remember, 2: Understand, 3: Apply) at which the attribute is assessed and *y* is the academic level (1: Beginner, 2: Intermediate, 3: Advanced) at which the attribute is assessed.

Topics and Specific Learning Objectives

1. **Introduction to Information Security**

   At the end of this section, students will be able to:

   a. Define our essential security goals: confidentiality, integrity and authenticity,

   b. Motivate basic security principles (Kerckhoff's principle, don't-roll-your-own, etc),

   c. Differentiate between formal security definitions: IND-EAV, IND-CPA, IND-CCA and IND-CCA2.

   d. Be able to perform basic security analysis of an encryption scheme to decide if it meets a given security definition or not.

2. **Symmetric Key Encryption**

   At the end of this section, students will be able to:

a. Explain the security properties of ideal block ciphers and stream ciphers,

b. Be able to select appropriate block cipher modes of operation (e.g., CBC, CTR, etc),

c. Understand the basic workings of commonly used symmetric-key ciphers (e.g., AES).

3. **Hash Functions and Message Authentication Codes**

   At the end of this section, students will be able to:

   a. Explain the security properties of hash functions and message authentication codes, and understand their role in security applications.

   b. Understand the basic inner workings of common hash functions (i.e., the SHA family).

   c. Understand the purpose of authenticated encryption (e.g., AES-GCM).

4. **Public Key Encryption**

   At the end of this section, students will be able to:

   a. Comprehend the basic mathematics behind common public-key families: RSA, discrete logarithm, and elliptic curve cryptography,

   b. Understand the steps and security properties of the Diffie-Hellman public-key agreement protocol (e.g., DHE, ECDHE), and digital signatures (e.g., RSA, ECDSA).

5. **Entropy and Key Generation**

   At the end of this section, students will be able to:

   a. Understand the basics of random and pseudo-random bit generation,

   b. Be able to pick appropriate key lengths for the various primitives described above.

6. **Password Generation and Storage**

   At the end of this section, students will be able to:

   a. Understand the security requirements of passwords and explain common strategies for generating them (system assigned vs. user chosen, key stretching, etc.),

   b. Understand the security requirements of password databases and explain concepts associated with their implementation (e.g., password hashing, salting, etc.).

7. **Digital Certificates and Public Key Infrastructures**

   At the end of this section, students will be able to:

   a. Understand the security requirements and of digital certificates and explain the role of the various fields,

   b. Understand how certificates are generated, checked and revoked,

   c. Explain how an internet browser, mobile app, or device authenticates the identify of a server through a public key infrastructure.

8. **Transport Layer Security (TLS)**

   At the end of this section, students will be able to:

   a. Be able to describe the steps of the TLS 1.3 and 1.2 handshake protocols, and explain how these protocols use cryptographic primitives described above to guarantee confidentiality, integrity and authenticity,

   b. Be able to articulate some of the weaknesses of TLS 1.2, and explain how TLS 1.3 addresses them.

c. Be able to generate digital certificates and certificate signing requests,

d. Be able to correctly configure a TLS implementation including selecting appropriate ciphersuites and other settings.

e. Be able to test a webserver for correct TLS configuration.

Evaluation

Course Component	Weight
Assignments	30%
Midterm Test	20%
Final Examination	50%

To obtain a passing grade in the course, a mark of 50% or more must be achieved on the final examination. A final examination or laboratory mark < 50% will result in a final course grade of 48% or less.

Homework Assignments: There will be a maximum of 3 assignments, which will be submitted electronically via OWL. Specific instructions and due dates will appear in the assignment. Email submissions are not accepted.

Midterm Test: The midterm test will be closed book and use of electronic devices is not permitted.

Final Examination: The final examination will take place during the regular examination period. The final examination will be closed book and use of electronic devices is not permitted.

Late Submission Policy: Assignments are due at 23:59 (Eastern Time) on their respective due dates. The assignment submission form in OWL will be configured to accept submissions *up to 48 hours* past the original due date. There is no mark deduction for submitting during the 48-hour grace period, however course personnel will not give assistance with assignments after their original due date. Following the 48-hour grace period, OWL will no longer accept submissions, and a mark of *zero* (0) will be recorded for any un-submitted assignments.

Use of English: In accordance with Senate and Faculty Policy, students may be penalized up to 10% of the marks on all assignments, tests, and examinations for improper use of English. Additionally, poorly written work with the exception of the final examination may be returned without grading. If resubmission of the work is permitted, it may be graded with marks deducted for poor English and/or late submission.

Attendance: Any student who, in the opinion of the instructor, is absent too frequently from class, laboratory, or tutorial periods will be reported to the Dean (after due warning has been given). On the recommendation of the department, and with the permission of the Dean, the student will be debarred from taking the regular final examination in the course.

Absence Due to Illness or Other Circumstances: Students should immediately consult with the instructor or department Chair if they have any problems that could affect their performance in the

course. Where appropriate, the problems should be documented (see the attached "Instructions for Students Unable to Write Tests or Examinations or Submit Assignments as Scheduled"). The student should seek advice from the instructor or department Chair regarding how best to deal with the problem. Failure to notify the instructor or department Chair immediately (or as soon as possible thereafter) will have a negative effect on any appeal.

For more information concerning medical accommodations, see the relevant section of the Academic Handbook:
http://www.uwo.ca/univsec/pdf/academic_policies/appeals/accommodation_medical.pdf

For more information concerning accommodations for religious holidays, see the relevant section of the Academic Handbook:
http://www.uwo.ca/univsec/pdf/academic_policies/appeals/accommodation_religious.pdf

Missed Midterm Examinations: If a student misses a midterm examination, the exam will not be rescheduled. The student must follow the Instructions for Students Unable to Write Tests and provide documentation to their department within 24 hours of the missed test. The department will decide whether to allow the reweighting of the test, where reweighting means the marks normally allotted for the midterm will be added to the final exam. If no reasonable justification for missing the test can be found, then the student will receive a mark of zero for the test.

If a student is going to miss the midterm examination for religious reasons, they must inform the instructor in writing within 48 hours of the announcement of the exam date or they will be required to write the exam.

Cheating and Plagiarism: Students must write their essays and assignments in their own words. Whenever students take an idea or a passage from another author, they must acknowledge their debt both by using quotation marks where appropriate and by proper referencing such as footnotes or citations. University policy states that cheating, including plagiarism, is a scholastic offence. The commission of a scholastic offence is attended by academic penalties, which might include expulsion from the program. If you are caught cheating, there will be no second warning.

All required papers may be subject to submission for textual similarity review to commercial plagiarism-detection software under license to the University for the detection of plagiarism. All papers submitted will be included as source documents on the reference database for the purpose of detecting plagiarism of papers subsequently submitted to the system. Use of the service is subject to the licensing agreement, currently between the University of Western Ontario and Turnitin.com (http://www.turnitin.com).

Scholastic offences are taken seriously, and students are directed to read the appropriate policy, specifically, the definition of what constitutes a Scholastic Offence, in the relevant section of the Academic Handbook:
http://www.uwo.ca/univsec/pdf/academic_policies/appeals/scholastic_discipline_undergrad.pdf

Use of Electronic Devices: Students may use laptops, tablet computers, or smart phones *only* to access the course website during lectures and tutorials. No other electronic devices may be used at any time during tests or examinations.

Policy on Repeating All Components of a Course: Students who are required to repeat an Engineering course must repeat all components of the course. No special permissions will be granted enabling a student to retain laboratory, assignment, or test marks from previous years. Previously completed assignments and laboratories cannot be resubmitted by the student for grading in subsequent years.

Internet and Electronic Mail: Students are responsible for regularly checking their Western e-mail and the course web site: whisperlab.org/security and making themselves aware of any information that is posted about the course.

Accessibility: Please contact the course instructor if you require material in an alternate format or if any other arrangements can make this course more accessible to you. You may also wish to contact Services for Students with Disabilities (SSD) at 519-661-2111 ext. 82147 for any specific question regarding an accommodation.

Support Services: Office of the Registrar, http://www.registrar.uwo.ca/
Student Development Centre, http://www.sdc.uwo.ca/
Engineering Undergraduate Services, http://www.eng.uwo.ca/undergraduate/
USC Student Support Services, http://westernusc.ca/services/

Students who are in emotional/mental distress should refer to Mental Health @ Western, http://www.health.uwo.ca/mental_health/, for a complete list of options about how to obtain help.

INSTRUCTIONS FOR STUDENTS UNABLE TO WRITE TESTS OR EXAMINATIONS OR SUBMIT ASSIGNMENTS AS SCHEDULED

If, on medical or compassionate grounds you are unable to write term tests or final examinations or complete course work by the due date, you should follow the instructions listed below. You should understand that academic relief will not be granted automatically on request. You must demonstrate to your department (or the Undergraduate Services Office) that there are compelling medical or compassionate grounds that can be documented before academic relief will be considered. Different regulations apply to term tests, final examinations and late assignments. Please read the instructions carefully.

A. *GENERAL REGULATIONS & PROCEDURES*

1. All first year students will report to the Undergraduate Services Office, SEB 2097, for all instances.

2. If you are an upper year student and you are missing a test/assignment/lab or examination that is worth LESS THAN 10% of your mark, you should report to your department office to request relief. If your course work is MORE THAN 10% of your final grade, you will report to the Undergraduate Services Office, SEB 2097.

3. Check the course outline to see if the instructor has a policy for missed tests, examinations, late assignments or attendance.

4. Documentation must be provided as soon as possible. If no one is available in your department office or the Undergraduate Services Office, leave a message clearly stating your name & student number and reason for your call. The department telephone numbers are given at the end of these instructions.

5. If you decide to write a test or an examination you should be prepared to accept the mark you earn. Rewriting tests or examinations or having the value of a test or examination reweighted on a retroactive basis is not permitted.

B. *TERM TESTS*

1. If you are in first year and you are unable to write a term test, contact the Undergraduate Services Office, SEB 2097 PRIOR to the scheduled date of the test.

2. If you are an upper year student and you are unable to write a term test, inform your instructor PRIOR to the scheduled date of the test. If the instructor is not available, leave a message for him/her at the department office. If the test is worth LESS THAN 10% of your mark, you should report to your department office to request relief. If the test is worth MORE THAN 10% of your final grade you will report to the Undergraduate Services Office, SEB 2097 to request relief.

3. Be prepared to provide supporting documentation to the Department Chair and/or the Undergraduate Services Office (see next page for information on documentation).

4. Discuss with the instructor if and when the test can be rescheduled. **N.B.** The approval of the Chair or the Undergraduate Services Office is required when rescheduling term tests.

C. *FINAL EXAMINATIONS*

1. If you are unable to write a final examination, contact the Undergraduate Services Office PRIOR TO THE SCHEDULED EXAMINATION TIME to request permission to write a Special Final Examination. If no one is available in the Undergraduate Services Office, leave a message clearly stating your name & student number.

2. Be prepared to provide the Undergraduate Services Office with supporting documentation (see next page for information on documentation) the next day, or as soon as possible (in cases where students are hospitalized). The following circumstances are not considered grounds for missing a final examination or requesting special examinations: common cold, sleeping in, misreading timetable and travel arrangements.

3. In order to receive permission to write a Special Examination, you must obtain the approval of the Chair of the Department **and** the Associate Dean and in order to apply you must sign a "Recommendation for a Special Examination Form" available in the Undergraduate Services Office. The Undergraduate Services Office will then notify the course instructor(s) and reschedule the examination on your behalf.

   PLEASE NOTE: **It is the student's responsibility to check the date, time and location of the Special Examination.**

D. ***LATE ASSIGNMENTS***

1. Advise the instructor if you are having problems completing the assignment on time (**prior** to the due date of the assignment).
2. Be prepared to provide documentation if requested by the instructor (see reverse side for information on documentation).
3. If you are granted an extension, establish a due date. The approval of the Chair of your Department (or the Assistant Dean, First Year Studies, if you are in first year) is not required if assignments will be completed prior to the last day of classes.
4. i) Extensions beyond the end of classes must have the consent of the instructor, the department Chair and the Associate Dean, Undergraduate Studies. Documentation is mandatory.
   ii) A Recommendation of Incomplete Form must be filled out indicating the work to be completed and the date by which it is due. This form must be signed by the student, the instructor, the department Chair and the Associate Dean, Undergraduate Studies.

E. ***SHORT ABSENCES***

If you miss a class due to a minor illness or other problem, check your course outlines for information regarding attendance requirements and make sure you are not missing a test, laboratory or assignment. Cover any readings and arrange to borrow notes from a classmate.

F. ***EXTENDED ABSENCES***

If you are absent more than one week or if you get too far behind to catch up, you should consider reducing your workload by dropping one or more courses. (Note drop deadlines listed below). You may want to seek advice from your academic counsellor in the Undergraduate Services Office.

G. ***DOCUMENTATION***

If you consulted an off-campus doctor or Student Health Services regarding your illness or personal problem, **you must provide the doctor with a Student Medical Certificate** to complete at the time of your visit and then bring it to the Department (or the Undergraduate Services Office). **This note must contain the following information: severity of illness, effect on academic studies and duration of absence. Regular doctor's notes will not be accepted; only the Student Medical Certificate will be accepted.**

In Case of Serious Illness of a Family Member: Provide a Student Medical Certificate to your family member's physician to complete and bring it to the Department (or the Undergraduate Services Office if you are in first year).

In Case of a Death: Obtain a copy of the death certificate or the notice provided by the funeral director's office. You must include your relationship to the deceased and bring it to the Department (or the Undergraduate Services Office if you are in first year).

For Other Extenuating Circumstances: If you are not sure what documentation to provide, ask the Departmental Office (or the Undergraduate Services Office if you are in first year) for direction.

Note: Forged notes and certificates will be dealt with severely. To submit a forged document is a scholastic offence (see below).

H. ***ACADEMIC CONCERNS***

1. You need to know if your instructors have a policy on late penalties, missed tests, etc. This information may be included on the course outlines. If not, ask your instructor(s).

2. **You should also be aware of attendance requirements in some courses. You can be debarred from writing the final examination if your attendance is not satisfactory.**

3. If you are in academic difficulty, check out the minimum requirements for progression in the calendar. If in doubt, see your academic counsellor.

Calendar References: Check these regulations in your 2018 Western Academic Calendar available at www.westerncalendar.uwo.ca.

Absences Due to Illness:
http://www.westerncalendar.uwo.ca/PolicyPages.cfm?Command=showCategory&PolicyCategoryID=1&SelectedCalendar=Live&ArchiveID=#Page_12
Academic Accommodations for Students with Disabilities:
http://www.westerncalendar.uwo.ca/PolicyPages.cfm?Command=showCategory&PolicyCategoryID=1&SelectedCalendar=Live&ArchiveID=#Page_10
Academic Accommodations for Religious or Holy Days:
http://www.westerncalendar.uwo.ca/PolicyPages.cfm?Command=showCategory&PolicyCategoryID=1&SelectedCalendar=Live&ArchiveID=#Page_16
Course Withdrawals:
http://www.westerncalendar.uwo.ca/PolicyPages.cfm?Command=showCategory&PolicyCategoryID=6&SelectedCalendar=Live&ArchiveID=#Page_75
Examinations:
http://www.westerncalendar.uwo.ca/PolicyPages.cfm?PolicyCategoryID=5&command=showCategory&SelectedCalendar=Live&ArchiveID=
Scheduling of Term Assignments:
http://www.westerncalendar.uwo.ca/PolicyPages.cfm?Command=showCategory&PolicyCategoryID=5&SelectedCalendar=Live&ArchiveID=#SubHeading_78
Scholastic Offences:
http://www.westerncalendar.uwo.ca/PolicyPages.cfm?Command=showCategory&PolicyCategoryID=1&SelectedCalendar=Live&ArchiveID=#Page_20
Student Medical Certificate: https://www.eng.uwo.ca/files/undergraduate/forms/smc.pdf
Engineering Academic Regulations:
http://www.westerncalendar.uwo.ca/PolicyPages.cfm?Command=showCategory&PolicyCategoryID=4&SelectedCalendar=Live&ArchiveID=#Page_86

Note: These instructions apply to all students registered in the Faculty of Engineering regardless of whether the courses are offered by the Faculty of Engineering or other faculties in the University.

Add Deadlines:	First term half course (i.e. “A” or “F”)	September 14, 2018
	Full courses and full-year half course (i.e. “E”, “Y” or no suffix)	September 14, 2018
	Second term half course (i.e. “B” or “G”)	January 15, 2019
***Drop Deadlines*:**	First term half course (i.e. “A” or “F”)	November 12, 2018
	Full courses and full-year half courses (i.e. “E”,“Y” or no suffix)	November 30, 2018
	Second term half or second term full course (i.e. “B” or “G”)	March 7, 2019

Contact Information:

Undergraduate Services Office:	SEB 2097	Telephone: (519) 661-2130	E-mail: engugrad@uwo.ca
Dept. of Chemical and Biochemical Engineering & Green Process Engineering:	TEB 477	Telephone: (519) 661-2131	E-mail: cbeugrad@uwo.ca
Dept. of Civil and Environmental Engineering:	SEB 3005	Telephone: (519) 661-2139	E-mail: civil@uwo.ca
Dept. of Electrical and Computer Engineering, Software Engineering & Mechatronics Engineering:	TEB 279	Telephone: (519) 661-3758	Email: eceugrad@uwo.ca
Dept. of Mechanical and Materials Engineering:	SEB 3002	Telephone: (519) 661-4122	E-mail: mmeundergraduate@uwo.ca

Revised 08/01/18