Western University
Faculty of Engineering
Department of Electrical and Computer Engineering

SE 4472a / ECE 9064a: Information Security

Course Outline 2016-17

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: essex.cc/security
Consultation/office hour: TBD.

Academic Calendar Copy: http://westerncalendar.uwo.ca/2016/pg960.html#36494

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:

- 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. Explain the difference between public-key encryption (e.g. RSA), public-key agreement (e.g., ECDHE), and digital signatures (e.g., RSA, ECDSA), and understand their respective roles in security applications.

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. **TLS and SSH**

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

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

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

   c. Be able to correctly configure a TLS implementation including selecting appropriate ciphersuites. 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 be 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: http://essex.cc/teaching/Information-Security/ (or essex.cc/security for short) 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.