Western Engineering

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

SE 4472 – Information Security

Course Outline

Fall 2024

COURSE 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.
- **Digital Identity and Access Control:** Authentication and authorization, digital certificates (certificate chains, trust stores), secure password generation and storage.
- **Cryptographic Network Protocols:** TLS connections (handshake, ciphersuite agreement, establishing session keys). Public key infrastructure issues (issuing, checking and revoking certificates).

ACADEMIC CALENDAR:
https://www.westerncalendar.uwo.ca/Courses.cfm?CourseAcadCalendarID=MAIN_017915_1

PREREQUISITES: 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.

CEAB ACADEMIC UNITS: Engineering Science 75%, Engineering Design 25%.

INSTRUCTOR INFORMATION:

Name: Aleksander Essex

Office: TEB 234

Office Hour: After class or by appointment

Email: aessex@uwo.ca

CONTACT HOURS:

Timetable information is available at https://draftmyschedule.uwo.ca/.

Lectures occur weekly starting September 5th. Tutorial sessions occur weekly starting September 16th.

LECTURE:	**Tuesdays** 11:30am-12:30pm and **Thursdays** 1:30-3:30pm
TUTORIAL:	**Mondays** 10:30am-12:30pm

RECOMMENDED TEXT:

- Paul van Oorschot. Computer Security and the Internet: Tools and Jewels. Springer, 2020. ISBN: 978-3-030-33648-6.

Available for download from the university library through Springer Link:

https://link-springer-com.proxy1.lib.uwo.ca/book/10.1007/978-3-030-33649-3

RECOMMENDED RESOURCES/REFERENCES: IF APPLICABLE

- E. Rescorla. **The Transport Layer Security (TLS) Protocol Version 1.3.** RFC 8446. Available online: https://tools.ietf.org/html/rfc8446
- 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
- 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/

GENERAL LEARNING OBJECTIVES (CEAB GRADUATE ATTRIBUTES)

Knowledge Base	A	Engineering Tools		Impact on Society	A
Problem Analysis	D	Individual & Teamwork		Ethics and Equity	
Investigation	A	Communication		Economics and Project Mgmt.	
Design	A	Professionalism		Life-Long Learning	A

Notation: x represents the content level code as defined by the CEAB. blank = not applicable; I = introduced (introductory); D = developed (intermediate) and A = applied (advanced).

Rating: I – The instructor will introduce the topic at the level required. It is not necessary for the student to have seen the material before. D – There may be a reminder or review, but the student is expected to have seen and been tested on the material before taking the course. A – It is expected that the student can apply the knowledge without prompting (e. g. no review).

COURSE MATERIALS: Weekly lecture notes will be available on the external course site at: https://whisperlab/org/security. The material for this course will be taught in both lectures and tutorials; therefore, it is imperative that you attend each lecture and tutorial.

UNITS: SI

COURSE TOPICS AND SPECIFIC LEARNING OUTCOMES: The following table summarizes the course learning outcomes along with CEAB GAIs where the GAIs in bold indicate ones to be measured and reported annually.

COURSE TOPICS AND SPECIFIC LEARNING OUTCOMES	(CAEB) Graduate Attribute
1**. Course intro. Security goals and principles, secret keys, brute force guessing, bits of security** a. Define essential security goals (confidentiality, integrity and authenticity) b. Define basic security notions (brute force guessing, bits of security) **c.** Justify basic security principles (Kerckhoff's principle, don't-roll-your-own)	
2. Thinking Securely. Classical ciphers, formal security notions, attack games a. Differentiate between formal security definitions: IND-EAV, IND-CPA, IND-CCA and IND-CCA2. **b.** Be able to perform basic security analysis of an encryption scheme to decide if it meets a given security definition or not	**PA3, I1,** KB3, PA2
3. Encrypting data. Pseudo-random permutations, block ciphers, AES, cipher modes of operation, message padding a. Explain the security properties of ideal block ciphers, initialization vectors (IVs), and message padding b. Be able to select appropriate block cipher modes of operation (e.g., CBC, CTR, etc.) and appropriate key/IV lengths to provide the required security properties **c.** Understand the basic workings of commonly used symmetric-key ciphers (e.g., AES)	**PA1**
4. Fingerprinting data. Random oracles, hash functions, the SHA family, birthday paradox, collisions, pre-image and second-preimage resistance a. Explain the security properties of ideal hash functions and understand their purpose in security applications b. Be able to select appropriate hash functions and output lengths to provide the required security properties **c.** Understand the basic workings of commonly used hash functions (e.g., SHA-256)	

5. Authenticating data. Message authentication, message authentications codes, authenticated encryption, AES-GCM a. Explain the security properties of message authentication codes (MACs) and authenticated encryption (AE) and understand their purpose in security applications b. Be able to select appropriate MACs and AEs and key/IV lengths provide the required security properties c. Understand the basic workings of commonly used AEs (e.g., AES-GCM)	**IESE1**
6. Bootstrapping a shared secret. Public-key cryptography, public-key agreement, Diffie-Hellman a. Comprehend the basic mathematics behind the Diffie-Hellman protocol **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)	**KB1**
7. Linking data to a public key. Digital signatures, forgeries, RSA signatures and padding. a. Comprehend the basic mathematics behind RSA signatures b. Explain the security properties of digital signatures, and message padding **c.** Demonstrate the ability to create signature forgeries in insecure signatures schemes, and apply solutions to make it secure	
8. Linking a public key to an identity. Digital certificates, X509 a. The *trust-on-first-use* trust model. The Secure Shell (SSH) protocol **b.** Understand the security requirements and of digital certificates and explain the role of the various fields	
9. Server authentication. Public-key infrastructure, certificate authorities, revocation, pinning, trust stores a. Understand how certificates are generated, checked and revoked, **b.** Explain how an internet browser, mobile app, or device authenticates the identify of a server through a public key infrastructure	KB4
10. Securing the Transport Layer. The Transport Layer Security (TLS) 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 correctly configure a TLS implementation including selecting appropriate candidate ciphersuites and other settings	

c. Be able to test a webserver for correct TLS configuration	
11. Client authentication. Secure password generation and storage. Federated identity and single sign-on a. Explain the security properties of password hashing and salting b. Be able to select appropriate password generation and storage strategies to provide the required security properties	**D3**
12. Selected Topic in Cybersecurity	LL1

EVALUATION:

Name	**% Worth**	**Assigned**	**Due Date**	**CEAB GAs ASSESSED**
Assignment 1	5%	Sept. 12th	Sept. 20th	**I1**
Assignment 2	5%	Sept. 26th	Oct. 4th	**PA1**
Assignment 3	5%	Oct. 10th	Oct. 25th	
Assignment 4	5%	Nov. 7th	Nov. 15th	
Assignment 5	5%	Nov. 21st	Nov. 29th	
Mid-Term Examination	25%	n/a	Oct. 21st	**PA3, IESE1**
Final Examination	50%	n/a	TBA	**KB1, D3**

Note that the dates listed above are **tentative** and may be adjusted if needed. Marks will be assigned on the basis of method of analysis and presentation, correctness of solution, clarity and neatness.

COURSE POLICIES

TUTORIAL SESSIONS: Tutorial sessions are used to (a) discuss assignments, (b) answer student questions, (c) go through problems, and (d) go through the solutions to assignments and midterm. Solutions will not be posted separately. Therefore, attendance in the tutorials is essential. Students seeking special permission to miss the tutorial on an ongoing basis due to a

course conflict are expected to arrange with another class member or study group to share/discuss solutions.

ASSIGNMENTS: There will be five assignments, which will be submitted electronically via Gradescope. Email submissions are not accepted.

MIDTERM EXAMINATION: The midterm will be held **in person** during one of the weekly tutorial sessions at a location to be determined. It will be 1 hour long and will be **closed-book** (no notes, devices or devices).

FINAL EXAM: The final exam will be held **in person** at a date and location to be determined by the Registrar's Office. It will be 2 hours long and will be **closed-book** (no notes, devices or calculators).

LATE SUBMISSION POLICY: This course employs flexible deadlines for assignments. Each assignment is due at 11:59pm on the respective date found above in the course outline. Students are expected to submit the assignment by the deadline listed. Should illness or extenuating circumstances arise, students can submit their assignments past the deadline without academic penalty.

Assignment solutions will be taken up in the following week's tutorial session. In fairness to other students, a late assignment will not be accepted after the tutorial session begins. Unsubmitted assignments will receive a mark of zero (0). There are no make-up assignments or other extra-credit opportunities for unsubmitted assignments.

Example: Assignment 1 is due at 11:59 pm on Friday, September 20th. The following week's tutorial begins at 10:30 am on Monday, September 23rd. Assignment 1 will be accepted without academic penalty until then but will not be accepted after that.

As flexible deadlines are used in this course, requests for academic consideration will not be granted.

ATTENDANCE: Attendance is mandatory for all lectures and tutorials.

ABSENCE FROM MANDATORY COURSE COMMITMENTS: Students must familiarize themselves with the Policy on **Academic Consideration for Absences:**
https://www.eng.uwo.ca/undergraduate/academic-consideration-for-absences.html

I. **Missed/Late Accommodation Policy**

1. The Academic Consideration Request Form is available through the STUDENT ABSENCE PORTAL.
2. Documentation must be provided as soon as possible. Requests for academic consideration must include the following components:
   a. Indication of the course(s) and assessment(s) affected by the request
   b. Medical note, and
   c. Additional supporting documentation as relevant
3. Requests for academic consideration without a medical note or other supporting documentation may be accepted once per term, per course.

4. Undocumented absences cannot be used for examinations scheduled by the Office of the Registrar during official examination periods (including take-home final exams and December mid-year exams for full courses) and practical laboratory and performance tests typically scheduled in the last week of the term. Undocumented absences also cannot be used for the "designated assessment" in each course. When flexibility in assessment exists and is clearly stated on the course outline, both undocumented absences and academic consideration requests with documentation may be denied.
5. Forged notes and certificates will be dealt with severely. To submit a forged document is a scholastic offence.

II. Exam Accommodation

1. If you are unable to write a final examination, report your absence using the Academic Consideration Request Form through STUDENT ABSENCE PORTAL.
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, headache, 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 submit an the Academic Consideration Request Form through STUDENT ABSENCE PORTAL.
   PLEASE NOTE: It is the student's responsibility to check the date, time and location of the Special Examination.

III. LATE ASSIGNMENTS

IV. Medical Accommodation

1. Requests for Academic Consideration Request Form through STUDENT ABSENCE PORTAL.
2. Requests for academic consideration must include the following components:
   a. Self-attestation signed by the student (*This is only accepted for the first/one absence*)
   b. Medical note. Forged notes and certificates will be dealt with severely. To submit a forged document is a scholastic offence.
   c. Indication of the course(s) and assessment(s) affected by the request
   d. Supporting documentation as relevant
3. Requests without supporting documentation are limited to one per term per course.
4. **Students must request academic consideration as soon as possible and no later than 48 hours after the missed assessment.**
5. Once the request and supporting documents have been received and reviewed, appropriate academic consideration, if granted, shall be determined by the instructor in consultation with the academic advisor, in a manner consistent with the course outline.

   Academic consideration may include extension of deadlines, waiver of attendance requirements for classes/labs/tutorials, or re-weighting of course requirements. Some forms of academic consideration, such as arranging Special Examinations, assigning a grade of Incomplete, or granting late withdrawals without academic penalty, may only be granted by the Academic Advising office of the Faculty of Registration.

6. **An instructor may deny academic consideration for any assessment that is not required in the calculation of the final grade** (e.g., "8 of 10 quizzes"). Assessment flexibility must be indicated on the course outline.

7. **An instructor may deny academic consideration relating to the timeframe submission of work where there is already flexibility in the submission timeframe** (e.g., 72-hour submission window). This assessment flexibility must be indicated on the course outline.

V. Religious Accommodation

When scheduling unavoidably conflicts with religious holidays, which (a) require an absence from the University or (b) prohibit or require certain activities (i.e., activities that would make it impossible for the student to satisfy the academic requirements scheduled on the day(s) involved), no student will be penalized for absence because of religious reasons, and alternative means will be sought for satisfying the academic requirements involved. If a suitable arrangement cannot be worked out between the student and instructor involved, they should consult the appropriate Department Chair and, if necessary, the student's Dean.

It is the responsibility of such students to inform themselves concerning the work done in classes from which they are absent and to take appropriate action.

VI. Academic Integrity

In the Faculty of Engineering, we encourage students to create a culture of honesty, trust, fairness, respect, responsibility, and courage, befitting the professional degree you are pursuing.

Please visit Academic Integrity Western Engineering for more information

VII. Academic Offences

Plagiarism means using another's work without giving credit. The university has rules against plagiarism and other scholastic offences. Western Engineering has a zero-tolerance policy on plagiarism. The minimum penalty is zero on the course work and a repeat offence will earn you zero on the course. A third offence may lead to expulsion from the university.
Scholastic Discipline for Undergraduate Students & Cheating, Plagiarism and Unauthorized Collaboration: What Students Need to Know

Students must write their reports, 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

VIII. Faculty of Engineering AI Policy

The use of generative Artificial intelligence (GenAI) tools won't be discouraged in the Faculty of Engineering. As we pride ourselves on building the future we can't hide from the use of GenAI tools to contribute to the understanding of the course materials. However, the use of GenAI tools in any assignment or contribution during the course will have to be disclosed, as a resource.

GenAI tools use won't be permitted in any type of examination or other assessments where the faculty have prohibited their use. If use of GenAI tools is detected by the instructor in these instances, academic offences penalties might be imposed against the student.

IX. Use of English Policy

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 except for 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.

X. Accessibility

Western is committed to achieving barrier free accessibility for persons with disabilities studying, visiting and working at Western. As part of this commitment, there are a variety of services, groups and committees on campus devoted to promoting accessibility and to ensuring that individuals have equitable access to services and facilities. To help provide the best experience to all members of the campus community, please visit the Accessibility Western University for information on accessibility-related resources available at Western.

Students with disabilities may arrange for academic accommodation at Western. For a more detailed explanation, please visit Academic Support & Engagement -Academic Accommodation.

XI. Inclusivity, Diversity, and Respect

The Faculty of Engineering at Western University is committed to creating equitable and inclusive learning environments that value diverse perspectives and experiences. We recognize that university courses often marginalize students based on social identity characteristics such as, but not limited to, Indigeneity, race, ethnicity, nationality, ability, gender identity, gender expression, sexuality, age, language, religion, and socioeconomic status. Understanding this, we strive to facilitate equitable experiences and inclusion within the classroom by respecting and integrating multiple ways of knowing, being, and doing. Please visit the Office of Equity, Diversity and Inclusion.

XII. Health and Well-Being

- Health & Wellness Services – Students - Offers appointment-based medical clinic for all registered part-time and full-time students.
- Mental Health Support - Provides professional and confidential services, free of charge, to students needing assistance to meet their personal, social and academic goals. Services include consultation, referral, groups and workshops, as well as brief, change-oriented psychotherapy.
- Crisis Support - For immediate assistant, please visit Thames Hall Room 2170 or call 519-661-3030. The crisis clinic operates between 11:00 am - 4:30 pm. For after-hours crisis support, click here.
- Gender-Based Violence and Survivor Support - Western is committed to reducing incidents of gender-based and sexual violence and providing compassionate support to anyone who has gone through these traumatic events. If you have experienced gender-based or sexual violence (either recently or in the past), you will find information about support services for survivors, including emergency contacts, here. To connect with a case manager or set up an appointment, please contact support@uwo.ca.

Important Contacts

Engineering Undergraduate Services	SEB 2097	519-661-2130	engugrad@uwo.ca

Electrical and Computer Engineering	TEB 279	519-661-2111 x86264	eceugrad@uwo.ca
Office of the Registrar/Student Central	WSSB 1120	519-661-2100	

Important Links

- WESTERN ACADEMIC CALENDAR
- ACADEMIC RIGHTS AND RESPONSIBILITIES
- ENGINEERING PROGRESSION REQUIREMENTS AND ACADEMIC REGULATIONS
- UNIVERSITY STUDENTS' COUNCIL (USC) - SERVICES
- IMPORTANT DATES AND DEADLINES
- ACADEMIC CONSIDERATION FOR MEDICAL ILLNESS - UNDERGRADUATE STUDENTS
- ACCOMMODATIONS FOR RELIGIOUS HOLIDAYS
- SCHEDULING OF ASSIGNMENTS, TESTS, AND EXAMINATIONS
- STUDENT FORMS
- OFFICE OF THE REGISTRAR
- RETENTION OF ELECTRONIC VERSION OF COURSE OUTLINES (SYLLABI)
- ACADEMIC APPEALS
- STUDENT ABSENCE PORTAL