DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

SOFTWARE ENGINEERING

SE 4472 – INFORMATION SECURITY

Course Outline Fall 2025

COURSE DESCRIPTION: This course introduces the topic of information security in the context of network communication. It is intended for students who have some understanding of networks but no prior background in security. The goal of the course is to provide students with a foundation that will enable them to identify, analyze, and make informed 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).
- **Software Security:** An introduction to secure software design through the lens of memory safety in the C programming language.

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 Hours: After class or by appointment

Email: aessex@uwo.ca

CONTACT HOURS:

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

Lectures occur weekly starting Monday, September 8th. Tutorial sessions occur weekly starting Monday, September 15th.

LECTURE:	**Mondays** 3:30-4:30pm and **Wednesdays** 1:30-3:30pm
TUTORIAL:	**Mondays** 12:30-2:30pm

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

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: Students will develop knowledge and skills that allow them to take an integrated approach to reasoning about the security properties and requirements of cryptography in a network communication context.

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. Software security. Introduction to memory safety in the C programming language. a. Identify relevant virtual registers and regions of virtual memory b. Explain the mechanism of a stack buffer overflow	

EVALUATION:

Name	% Worth	Assigned	Due Date	CEAB GAs ASSESSED
Assignment 1	5%	Friday, Sept. 12th	Friday, Sept. 19th	**I1**
Assignment 2	5%	Friday, Sept. 26th	Friday, Oct. 3rd	**PA1**
Assignment 3	5%	Friday, Oct. 10th	Friday, Oct. 24th	
Assignment 4	5%	Friday, Nov. 7th	Friday, Nov. 14th	
Assignment 5	5%	Friday, Nov. 21st	Friday, Nov. 28th	
Mid-Term Examination	25%		Monday, Oct. 20th	**PA3, IESE1**
Final Examination	50%		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:
All work submitted must be of professional quality in the requested format. Material that is handed in dirty, illegible, disorganized, or in an unapproved format will be returned to the student for resubmission, and the late submission penalty will take effect. An additional penalty of 10% may be deducted for poor grammar, incoherence, or lack of flow in the written reports.

ASSIGNMENTS: There will be 5 assignments worth 5% each, which will be submitted online in Gradescope. Assignments are due at 11:55pm on the due date (listed above) but are subject to a flexible deadline (see Late Submission Policy below). Email submissions will not be accepted.

LECTURES: Attendance in the lecture sessions is mandatory; however, attendance is not formally tracked. Students who miss a lecture should consult the course lectures posted online.

TUTORIALS: Tutorials run every week. The tutorial sessions will be used to (1) discuss assignments and solution strategies, (2) take up solutions to completed assignments, (3) answer questions about the course material, and (4) hold the mid-term test. Electronic solutions to the assignments and midterm will not be provided; therefore, attendance in the tutorial sessions is essential for success in the course. Attendance in the tutorial sessions is mandatory; however, attendance is not formally tracked. Students who miss a tutorial session are expected to arrange with another classmate to obtain the tutorial notes.

MIDTERM TEST: A one-hour midterm test will take place during one of the weekly tutorial sessions. The specific examination room will be announced at a later date. The midterm is in-person and closed-book. No notes, calculators or electronic devices are permitted. The content of the test will be structured considering these factors. The test will consist of a mixed combination of multiple-choice and short-answer questions. The midterm is a designated assessment, meaning formal supporting documentation will be required for any student missing the midterm. A missed midterm will not be rescheduled. Instead, the mark value will be re-weighted into the final exam. For more information, consult Western's policies on academic consideration: https://registrar.uwo.ca/academics/academic_considerations/

FINAL EXAMINATION: A two-hour final exam will take place during the regular examination period. The final exam is in-person and closed-book. No notes, calculators or electronic devices are permitted. The content of the exam will be structured considering these factors. The exam will consist of a mixed combination of multiple-choice and short-answer questions. The course grade will be calculated based on performance in each of the course components listed above. The course does not require a passing grade on the final exam to pass the course.

LATE SUBMISSION POLICY:

This course employs flexible deadlines for assignments. The assignment deadlines can be found in the course outline above. For each assignment, students are expected to submit the assignment by the deadline listed. Should illness or extenuating circumstances arise, students are permitted to submit their assignment up to 48 hours (2 days) past the deadline without academic penalty.

The end of the 48-hour flexible submission grace period will coincide with a tutorial session, during which the assignment solutions will be discussed. In fairness to other students, the assignment submission website will not accept assignments 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.

As flexible deadlines are used in this course, requests for academic consideration will not be granted. If you have a long-term academic consideration or an accommodation for disability that allows greater flexibility than provided here, please reach out to your instructor at least one week before the posted deadline.

It is your responsibility (a) to know the assignment due dates, (b) to understand the course late submission policy, and (c) to manage your time appropriately, including building resilience in your schedule against unforeseen delays.

ATTENDANCE: Attendance is mandatory for all lectures and tutorials; however, attendance is not formally tracked. Please refer to the course policies above.

FACULTY OF ENGINEERING POLICIES:

Students must familiarize themselves with the policies of the Faculty of Engineering
https://www.eng.uwo.ca/electrical//pdf/2025-UG-Policy-and-Procedures.pdf