

**DEPARTMENT OF ELECTRICAL AND COMPUTER
ENGINEERING**

SE 4472A – INFORMATION SECURITY

Course Outline Fall 2026

COURSE DESCRIPTION: This course provides an introduction to the topic of security in the context of computer networks. The goals are to provide students with a foundation allowing them to identify, analyze, and solve network-related security problems in information systems with the emphasis on the engineering aspects of information security.

ACADEMIC CALENDAR:

[Link to Academic Calendar](#)

PREREQUISITES: ECE 4436A/B, SE 3313A/B (or CS 3357 A/B, CS 3305A/B)

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

INSTRUCTOR INFORMATION:

- **Name:**
- **Office Hours:**
- **E-mail:**

CONTACT HOURS:

- **Lecture:**
- **Tutorial:**

RECOMMENDED TEXT:

- P.C. Van Oorschot, *Computer Security and the Internet: Tools and Jewels*, 1st ed. 2020. Cham: Springer International Publishing, 2020. doi:10.1007/978-3-030-33649-3.

RECOMMENDED SOFTWARE:

- *Wireshark*. (ver. 4.6.8.). Wireshark Foundation. [Online]. Available: <https://www.wireshark.org>

RECOMMENDED RESOURCES/REFERENCES:

- E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," RFC 9846, RFC Editor, Jul. 2026, doi:10.17487/RFC9846. [Online]. Available: <https://www.rfc-editor.org/info/rfc9846/>

GENERAL LEARNING OBJECTIVES (CEAB GRADUATE ATTRIBUTES)

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

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: The material for this course will be taught in lectures every week and will be made available on OWL Brightspace. It is imperative that you attend each lecture and tutorial.

UNITS: SI

COURSE TOPICS AND SPECIFIC LEARNING OUTCOMES:

The course will allow students to develop the necessary skills and knowledge for identifying and analyzing security requirements for network communication systems, as well as configuring secure network communications. The following table summarizes the course topics and learning outcomes, along with the CEAB GAs where the GAs in bold indicate ones to be measured and reported annually.

COURSE TOPICS AND SPECIFIC LEARNING OUTCOMES	(CEAB) Graduate Attribute
Introduction to security concepts, goals and principles 1. Define essential security goals (confidentiality, integrity, authenticity, accountability) 2. Define basic security notions and concepts (brute force guessing, bits of security) 3. Justify basic security principles (Kerckhoff's principle)	
Formal security definitions and encryption schemes 1. Differentiate between formal security definitions: IND-EAV, IND-CPA, IND-CCA, and IND-CCA2 2. Perform basic security analysis of an encryption scheme to decide if it meets a given security definition or not	PA3, IN1, KB3, PA2
Data encryption: Block ciphers, AES, message padding, pseudo-random permutations 1. Explain the security properties of ideal block ciphers, message padding, and initialization vectors (IVs) 2. Select appropriate block cipher modes of operation (e.g., CBC, CTR) and appropriate key/IV lengths to provide the required security properties 3. Understand the functionality of commonly used symmetric-key ciphers (e.g., AES)	PA1
Data fingerprinting: hash functions, random oracles, collisions, birthday paradox, pre-image resistance 1. Explain the security properties of ideal block ciphers, message padding, and initialization vectors (IVs) 2. Select appropriate block cipher modes of operation (e.g., CBC, CTR) and appropriate key/IV lengths to provide the required security properties	
Digital authentication: message authentication, authenticated encryption, AES-GCM 1. Explain the security properties of message authentication codes (MACs) and authenticated encryption (AE) and understand their purpose in security applications 2. Select appropriate MACs and AEs given required security properties 3. Understand the functionality of commonly used AEs (e.g., AES-GCM)	IESE1

Public-key cryptography: Diffie-Hellman, public-key agreement, shared-secret bootstrapping 1. Understand and explain the operations behind the Diffie-Hellman protocol 2. Analyze the security properties and steps of the Diffie-Hellman public-key agreement protocol (e.g., DHE, ECDHE) and digital signatures (e.g., RSA, ECSAD)	KB1
Digital signatures, forgeries, RSA signatures and padding 1. Understand the mathematics behind RSA signatures 2. Explain the security properties of digital signatures and message padding 3. Demonstrate the ability to create signature forgeries in insecure signature schemes and apply solutions to make them secure	
Digital certificates, authenticity, X509 1. Analyze and assess the <i>trust-on-first-use</i> trust model 2. Understand the security requirements of digital certificates and identify their usage in various fields	
Digital authentication: public-key infrastructure, certificate authorities, revocation, pinning, trust stores 1. Understand the process of how digital certificates are generated, checked, and revoked 2. Explain how internet browsers, mobile applications, and devices authenticate the identity of a server through public-key infrastructure	KB4
Transport Layer Security (TLS) in modern networks 1. Describe the steps of the TLS 1.3 handshake protocol 2. Explain how TLS 1.3 uses cryptographic primitives to guarantee confidentiality, integrity, and authenticity security goals 3. Configure TLS in a network environment, including selecting appropriate candidate ciphersuites and other settings 4. Evaluate a web server for properly configured TLS implementation	
Client authentication: secure password generation and storage, federated identity, SSO 5. Understand the security properties of password hashing and salting	D3

6. Select appropriate password generation and storage strategies to provide required security properties	
Data privacy: ethics in digital forensic analysis 1. Understand the importance of evidence-production and lack of accountability 2. Observe and understand anomalous network activity in communication procedures to protect personal data access 3. Analyze a data privacy map for organizational data regulation, collection, retention	EE1

EVALUATION:

Name	% Worth	Assigned (Tentative)	Due Date (Tentative)	CEAB GAs ASSESSED
Assignment 1	5%			IN1
Assignment 2	5%			PA1
Assignment 3	5%			
Assignment 4	5%			
Assignment 5	5%			EE1
Midterm Examination	25%			PA3, IESE1

Final Examination	50%			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.

A course website will be maintained on OWL Brightspace. Assignments, submission deadlines, announcements for the course, and so on, will be posted on the website for electronic viewing and download.

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

LECTURES: Attendance in the lecture sessions is mandatory.

TUTORIALS: Tutorials run every week. Attendance in the tutorial sessions is strongly recommended for success in the course. The sessions will be used to discuss assignments and solution strategies, take up solutions to completed assignments, answer questions about course material, and hold the midterm examination. Electronic solutions to the assignments and midterm will not be provided.

MIDTERM EXAMINATION: A one-hour midterm examination 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 that 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, please consult [Western's policies](#) on academic consideration.

FINAL EXAMINATION: The final exam will take place during the regular examination period. The final exam will be two hours long, 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:

Advise the instructor if you are having problems completing the assignment on time prior to the due date of the assignment and be prepared to submit an Academic Consideration Request and provide documentation if requested by the instructor at: <https://www.eng.uwo.ca/undergraduate/academic-consideration-for-absences.html>. If you are granted an extension, establish a due date with the instructor. 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.

This course employs flexible deadlines for assignments. The assignment deadlines can be found above in the course outline. 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 past the deadline without academic penalty. Should students submit their assessment beyond 48 hours past the deadline, a late penalty of 20% per day will be subtracted from the assessed grade. **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 prior to the posted deadline.

ATTENDANCE: Attendance is mandatory for all lectures.

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>