UNSW Course Outline

TELE3119 Trusted Networks - 2024

Published on the 07 Sep 2024

General Course Information

Course Code : TELE3119
Year : 2024
Term : Term 3
Teaching Period : T3
Is a multi-term course? : No
Faculty : Faculty of Engineering
Academic Unit : School of Electrical Engineering & Telecommunications
Delivery Mode : In Person
Delivery Format : Standard
Delivery Location : Kensington
Campus : Sydney
Study Level : Undergraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

Information exchange via data communication networks is vulnerable to malicious intrusion. This course aims at students wishing to understand security issues in communication networks. It is designed to provide an integrated focus on security-related aspects of networking, as a core competency for telecommunications engineers.

The course content covers 3 areas: cryptography (Symmetric Encryption and Message Confidentiality, Public-Key Cryptography and Message Authentication, Key Distribution, Mathematical Principles of Cryptography), network security applications (Authentication Applications, Electronic Mail Security, IP Security, Web Security), and system security (Intruders, Attacks and Countermeasures, Malicious Software, Firewalls).

Course Aims

This course builds on concepts and principles introduced in TELE3118. More specifically, the course is intrinsically linked to the concepts, protocols, and networking fundamentals developed in TELE3118. The networking issues covered in TELE3118 are re-analysed from the standpoint of trust, authentication, integrity, and security. The aim is to provide students with a good understanding of the principles underlying trust and security in modern telecommunication networks and how to design such networks which is considered a paramount networking skill.

Course Learning Outcomes

Course Learning Outcomes
CLO1 : Explain the theory, concepts and challenges of encryption protocols
CLO2 : Explain the theory, concepts and challenges of authentication protocols
CLO3 : Explain how applications actually operate over communication networks
CLO4 : Explain key objectives in designing and analyzing a secured network
CLO5 : Design and simulate the behavior of security in communication networks
CLO6 : Design secure and trusted network applications, and design web-based applications running over Secure Sockets Layer
CLO7 : Design network authentication systems and possess the ability to analyze network traffic from a security standpoint

Course Learning Outcomes	Assessment Item
CLO1 : Explain the theory, concepts and challenges of encryption protocols	• Class Quizzes • Final Examination • Laboratory Assessment
CLO2 : Explain the theory, concepts and challenges of authentication protocols	• Class Quizzes • Final Examination • Laboratory Assessment
CLO3 : Explain how applications actually operate over communication networks	• Class Quizzes • Final Examination • Laboratory Assessment
CLO4 : Explain key objectives in designing and analyzing a secured network	• Class Quizzes • Final Examination • Laboratory Assessment
CLO5 : Design and simulate the behavior of security in communication networks	• Class Quizzes • Final Examination • Laboratory Assessment
CLO6 : Design secure and trusted network applications, and design web-based applications running over Secure Sockets Layer	• Final Examination • Laboratory Assessment
CLO7 : Design network authentication systems and possess the ability to analyze network traffic from a security standpoint	• Final Examination • Laboratory Assessment

Learning and Teaching Technologies

Moodle - Learning Management System | Microsoft Teams

Learning and Teaching in this course

Learning

- You are expected to attend all lectures, labs, and quizzes to maximise learning.
- In addition to the lecture notes, you should read relevant sections of the recommended reading material.
- Group learning is also encouraged. It is *assumed* that self-directed study of this kind is undertaken in addition to attending face-to-face classes throughout the course.

Teaching

- Lectures – to give the basic material, discuss the intuition behind the mathematics, and learn to incorporate rigour in the solution process.
- Tutorials – to learn problem-solving techniques, employ critical thinking, and reflect and discuss alternative techniques.
- Labs – laboratory assignments will provide hands-on experience of network security and an opportunity for constructing and evaluating practical tools.

Other Professional Outcomes

The learning outcoems of the cousre are:

LO1: Understand the theory, concepts, and challenges of encryption protocols

LO2: Understand the theory, concepts, and challenges of authentication protocols

LO3: A practical understanding of how applications operate over communication networks

LO4: Understand key objectives in designing and analyzing a secured network

LO5: Be able to design and simulate the behaviour of security in communication networks

LO6: Design secure and trusted network applications, and design web-based applications running over the Secure Sockets Layer

LO7: Design network authentication systems and possess the ability to analyze network traffic from a security standpoint.

Relationship to Engineers Australia Stage 1 competencies are as follows:

	PE1.1	PE1.2	PE1.3	PE1.4	PE1.5	PE1.6	PE2.1	PE2.2	PE2.3	PE2.4	PE3.1	PE3.2	PE3.3	PE3.4	PE3.5	PE3.6
LO1	X	x														
LO2	X	x	x	x												
LO3			x	x	x		x	x	x						x	
LO4			x				x	x	x		x	x	x		x	
LO5							x	x	x							
LO6						x	x	x	x			x				
LO7						x	x	x	x			x				

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
Class Quizzes Assessment Format: Individual	30%	Start Date: Week 4 and Week 7 Due Date: Not Applicable
Final Examination Assessment Format: Individual	40%	Start Date: Not Applicable Due Date: Not Applicable
Laboratory Assessment Assessment Format: Individual Short Extension: Yes (7 days)	30%	Start Date: Not Applicable Due Date: Not Applicable

Assessment Details

Class Quizzes

Assessment Overview

There are 2 forty-minute class quizzes, scheduled in week 4 and week 9, to help students receive timely feedback on their understanding of the course material covered so far. Each quiz is worth 15% of the final grade, and each will typically test students' problem-solving skills. Marks will be assigned according to the correctness of the responses. Class-wide feedback will be verbally given during a later lecture. Individual feedback will also be provided upon request.

Course Learning Outcomes

- CLO1 : Explain the theory, concepts and challenges of encryption protocols
- CLO2 : Explain the theory, concepts and challenges of authentication protocols
- CLO3 : Explain how applications actually operate over communication networks
- CLO4 : Explain key objectives in designing and analyzing a secured network
- CLO5 : Design and simulate the behavior of security in communication networks

Submission notes

On line

Assignment submission Turnitin type

Not Applicable

Generative AI Permission Level

Not Applicable

Generative AI is not considered to be of assistance to you in completing this assessment. If you do use generative AI in completing this assessment, you should attribute its use.

For more information on Generative AI and permitted use please see here.

Can use generative AI

Final Examination

Assessment Overview

This two-hour written examination aims to assess students' competency. Questions may be drawn from any aspect of the course unless specifically indicated otherwise by the lecturer. Marks will be assigned according to the correctness of the responses.

Course Learning Outcomes

- CLO1 : Explain the theory, concepts and challenges of encryption protocols
- CLO2 : Explain the theory, concepts and challenges of authentication protocols
- CLO3 : Explain how applications actually operate over communication networks
- CLO4 : Explain key objectives in designing and analyzing a secured network
- CLO5 : Design and simulate the behavior of security in communication networks
- CLO6 : Design secure and trusted network applications, and design web-based applications running over Secure Sockets Layer
- CLO7 : Design network authentication systems and possess the ability to analyze network traffic from a security standpoint

Assessment Length

On-line exam

Assignment submission Turnitin type

Not Applicable

Generative AI Permission Level

Not Applicable

Generative AI is not considered to be of assistance to you in completing this assessment. If you do use generative AI in completing this assessment, you should attribute its use.
For more information on Generative AI and permitted use please see here.

Can use generative AI

Laboratory Assessment

Assessment Overview

There are 4 experiments to be done over the three-hour weekly lab sessions with an oral

assessment at the end of each session. In addition, an oral lab exam will be conducted during the final week (week 10) lab session. Marks will be assigned according to the correctness of the responses and verbal feedback given by the demonstrators.

Course Learning Outcomes

- CLO1 : Explain the theory, concepts and challenges of encryption protocols
- CLO2 : Explain the theory, concepts and challenges of authentication protocols
- CLO3 : Explain how applications actually operate over communication networks
- CLO4 : Explain key objectives in designing and analyzing a secured network
- CLO5 : Design and simulate the behavior of security in communication networks
- CLO6 : Design secure and trusted network applications, and design web-based applications running over Secure Sockets Layer
- CLO7 : Design network authentication systems and possess the ability to analyze network traffic from a security standpoint

Assessment Length

Face to face assessement

Assignment submission Turnitin type

Not Applicable

Generative AI Permission Level

Not Applicable

Generative AI is not considered to be of assistance to you in completing this assessment. If you do use generative AI in completing this assessment, you should attribute its use.
For more information on Generative AI and permitted use please see here.

Generative AI can be used.

General Assessment Information

The assessment scheme in this course reflects the intention to assess your learning progress through the semester. Ongoing assessment occurs through the lab checkpoints (see lab manual), lab exams and the mid-semester exam.

Grading Basis

Standard

Requirements to pass course

Passing all the assessment tasks.

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 1 : 9 September - 15 September	Lecture	Basics of Cryptography 1 • Overview, Crypto Systems, Symmetric-Key Cryptography
Week 2 : 16 September - 22 September	Lecture	Basics of Cryptography 2 Asymmetric Cryptography
Week 3 : 23 September - 29 September	Lecture	Cryptography Infrastructure • Digital Signatures, Pretty Good Privacy, Public Key Infrastructure
Week 4 : 30 September - 6 October	Assessment	Monday, 30 September 2024 - Class Quiz 1
	Lecture	Applications 1 • Crypto Currencies • Internet Privacy
Week 5 : 7 October - 13 October	Lecture	Applications 2 • (Internet Privacy) • End-to-End Protocols (Signal)
Week 6 : 14 October - 20 October	Activity	Flexibility week Catch-up on Workshops and Labs. No Lectures
Week 7 : 21 October - 27 October	Assessment	Monday 21 October 2024 - Class Quiz 2
	Lecture	Securing Communications 1 • TLS/SSL, IPSec
Week 8 : 28 October - 3 November	Lecture	Securing Networked Systems • Firewall, Intrusion Detection Systems, VPNs
Week 9 : 4 November - 10 November	Lecture	Attacking Networked Systems • Data Exfiltration & Side Channel Attacks Warp up
Week 10 : 11 November - 17 November	Lecture	Attacking Networked Systems • Data Exfiltration & Side Channel Attacks Warp up

Attendance Requirements

Students are strongly encouraged to attend all classes and review lecture recordings.

Course Resources

Prescribed Resources

Will be provided each week

Recommended Resources

Will be provided each week.

Additional Costs

None

Course Evaluation and Development

This course is under constant revision to improve the learning outcomes for all students. Based

on feedback from past years we will endeavour to provide more support for the programming aspects of the lab work. Please forward any feedback (positive or negative) on the course to the course convener or via the online student survey MyExperience. As a result of previous feedback obtained for this course and in our efforts to provide a rich and meaningful learning experience, we have continued to evaluate and modify our delivery and assessment methods.

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
	Aruna Senevir atne					No	Yes

Other Useful Information

Academic Information

I. Special consideration and supplementary assessment

If you have experienced an illness or misadventure beyond your control that will interfere with your assessment performance, you are eligible to apply for Special Consideration prior to, or within 3 working days of, submitting an assessment or sitting an exam.

Please note that UNSW has a Fit to Sit rule, which means that if you sit an exam, you are declaring yourself fit enough to do so and cannot later apply for Special Consideration.

For details of applying for Special Consideration and conditions for the award of supplementary assessment, please see the information on UNSW's Special Consideration page.

II. Administrative matters and links

All students are expected to read and be familiar with UNSW guidelines and polices. In particular, students should be familiar with the following:

- Attendance
- UNSW Email Address
- Special Consideration
- Exams
- Approved Calculators
- Academic Honesty and Plagiarism

- Equitable Learning Services

III. Equity and diversity

Those students who have a disability that requires some adjustment in their teaching or learning environment are encouraged to discuss their study needs with the course convener prior to, or at the commencement of, their course, or with the Equity Officer (Disability) in the Equitable Learning Services. Issues to be discussed may include access to materials, signers or note-takers, the provision of services and additional exam and assessment arrangements. Early notification is essential to enable any necessary adjustments to be made.

IV. Professional Outcomes and Program Design

Students are able to review the relevant professional outcomes and program designs for their streams by going to the following link: https://www.unsw.edu.au/engineering/student-life/student-resources/program-design.

Note: This course outline sets out the description of classes at the date the Course Outline is published. The nature of classes may change during the Term after the Course Outline is published. Moodle or your primary learning management system (LMS) should be consulted for the up-to-date class descriptions. If there is any inconsistency in the description of activities between the University timetable and the Course Outline/Moodle/LMS, the description in the Course Outline/Moodle/LMS applies.

Academic Honesty and Plagarism

UNSW has an ongoing commitment to fostering a culture of learning informed by academic integrity. All UNSW students have a responsibility to adhere to this principle of academic integrity. Plagiarism undermines academic integrity and is not tolerated at UNSW. *Plagiarism at UNSW is defined as using the words or ideas of others and passing them off as your own.*

Plagiarism is a type of intellectual theft. It can take many forms, from deliberate cheating to accidentally copying from a source without acknowledgement. UNSW has produced a website with a wealth of resources to support students to understand and avoid plagiarism, visit: student.unsw.edu.au/plagiarism. The Learning Centre assists students with understanding academic integrity and how not to plagiarise. They also hold workshops and can help students one-on-one.

You are also reminded that careful time management is an important part of study and one of the identified causes of plagiarism is poor time management. Students should allow sufficient time for research, drafting and the proper referencing of sources in preparing all assessment tasks.

Repeated plagiarism (even in first year), plagiarism after first year, or serious instances, may also be investigated under the Student Misconduct Procedures. The penalties under the procedures can include a reduction in marks, failing a course or for the most serious matters (like plagiarism in an honours thesis or contract cheating) even suspension from the university. The Student Misconduct Procedures are available here:

www.gs.unsw.edu.au/policy/documents/studentmisconductprocedures.pdf

Submission of Assessment Tasks

Work submitted late without an approved extension by the course coordinator or delegated authority is subject to a late penalty of five percent (5%) of the maximum mark possible for that assessment item, per calendar day.

The late penalty is applied per calendar day (including weekends and public holidays) that the assessment is overdue. There is no pro-rata of the late penalty for submissions made part way through a day. This is for all assessments where a penalty applies.

Work submitted after five days (120 hours) will not be accepted and a mark of zero will be awarded for that assessment item.

For some assessment items, a late penalty may not be appropriate. These will be clearly indicated in the course outline, and such assessments will receive a mark of zero if not completed by the specified date. Examples include:

- Weekly online tests or laboratory work worth a small proportion of the subject mark;
- Exams, peer feedback and team evaluation surveys;
- Online quizzes where answers are released to students on completion;
- Professional assessment tasks, where the intention is to create an authentic assessment that has an absolute submission date; and,
- Pass/Fail assessment tasks.

Faculty-specific Information

Engineering Student Support Services – The Nucleus - enrolment, progression checks, clash

requests, course issues or program-related queries

Engineering Industrial Training – Industrial training questions

UNSW Study Abroad – study abroad student enquiries (for inbound students)

UNSW Exchange – student exchange enquiries (for inbound students)

UNSW Future Students – potential student enquiries e.g. admissions, fees, programs, credit transfer

Phone

(+61 2) 9385 8500 – Nucleus Student Hub

(+61 2) 9385 7661 – Engineering Industrial Training

(+61 2) 9385 3179 – UNSW Study Abroad and UNSW Exchange (for inbound students)

School-specific Information

General Conduct and Behaviour

Consideration and respect for the needs of your fellow students and teaching staff is an expectation. Conduct which unduly disrupts or interferes with a class is not acceptable and students may be asked to leave the class.

Use of AI for assessments

Your work must be your own. If you use AI in the writing of your assessment, you must acknowledge this and your submission must be substantially your own work. More information can be found on this website.

Workplace Health & Safety (WHS)

WHS for students and staff is of utmost priority. Most courses involve laboratory work. You must follow the rules about conduct in the laboratory. About COVID-19, advice can be found on this website.

School Contact Information

Consultations: Lecturer consultation times will be advised during the first lecture. You are welcome to email the tutor or laboratory demonstrator, who can answer your questions on this course and can also provide you with consultation times. ALL email enquiries should be made from your student email address with ELEC/TELExxxx in the subject line; otherwise they will not be answered.

Keeping Informed: Announcements may be made during classes, via email (to your student email address) and/or via online learning and teaching platforms – in this course, we will use Moodle https://moodle.telt.unsw.edu.au/login/index.php. Please note that you will be deemed to have received this information, so you should take careful note of all announcements.

Student Support Enquiries

For enrolment and progression enquiries please contact Student Services

Web

Electrical Engineering Homepage