UNSW Course Outline

COMP6841 Extended Security Engineering and Cyber Security - 2024

Published on the 25 Aug 2024

General Course Information

Course Code : COMP6841
Year : 2024
Term : Term 3
Teaching Period : T3
Is a multi-term course? : No
Faculty : Faculty of Engineering
Academic Unit : School of Computer Science and Engineering
Delivery Mode : In Person
Delivery Format : Standard
Delivery Location : Kensington
Campus : Sydney
Study Level : Postgraduate, Undergraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

In this introductory cybersecurity course we look at Security Engineering – the engineering

principles behind designing, monitoring, and maintaining security in the face of an adversary. We explore selected case studies and examine the practical principles behind effective security. We introduce the fundamental ideas of security and then we look at how these are applied in current cyber security practice. We will pay particular attention to systems which fail and the importance of thinking like an attacker. This course involves analysis, critical thinking and design. A cunning and devious mind will be an asset. Although our main concern is cybersecurity, the engineering principles we cover apply to security more generally.

This course introduces modern cybersecurity design and practice, and is suitable for anyone with a playful analytical mind and a general interest in security. We assume knowledge of coding, ideally in C, and knowledge of low level computing concepts such as memory implementation and function calling. The course provides an introduction to applied cyber security, as well as analytical skills and taking an engineering approach to security design. We'll also bring you up to date with the current main trends in cybersecurity.

In this course you will undertake an applied self directed security project.

There is an associated "Core" version of this course (COMP6441). CSE students will probably choose to take this Extended course rather than the core course, but are not required to. You can transfer between these two associated courses before the census date if you can't make up your mind in advance which is better for you.

This extended course is the core course plus additional applied technical material.

After completing COMP6841 you can proceed to the other UNSW Computing Security Courses covering topics in:

- Digital forensics
- Penetration testing
- Memory corruption and exploitation
- Software assurance
- Incident response
- Malware analysis and reversing
- Cryptanalysis
- Professional issues and leadership in security
- Web application security
- Special projects
- Masterclass

The precise topics covered in this course will change from year to year to keep the coverage up-

to-date and relevant. The field is now too big for us to cover everything in detail in a single course but by the end of this course you will have an overview of the major topics in contemporary security, a good understanding of the current state of the field, and have begun to think like a security engineer.

Our intention is to make this a highly enjoyable course. The field is quite stimulating as the security mindset you will develop involves understanding know how to break things in creative ways (as well as how to create things as is traditional in computing) with puzzles, cunning, cloak-and-dagger antics and a never-ending supply of amusing stories. However it will not be an easy course – you are expected to master the underlying theory *and* to be able to apply it to real world situations. There is a lot to learn and we expect you to work hard and study it in your own time.

Course Aims

There are 5 desired objectives of this course:

1. Think like a security engineer
2. Cybersecurity literacy

3. Cryptographic literacy

4. Applied security technical skills (introductory level)
5. Security engineering professional skills

Relationship to Other Courses

Taught in conjuntion with COMP6441 (Extended Security Engineering), with two common lectures and common security analysis case studies.

Taught in conjunction with LAWS3040 (Regulation for Cyber Security), with one common lecture and common security analysis case studies.

Course Learning Outcomes

Course Learning Outcomes
CLO1 : Make reasonable assessments of likely future trends and emerging risks in cyber security, based on an understanding of the historical context and current developments in the field
CLO2 : Demonstrate an understanding of the relationship of cyber security to related fields including safety science, psychology, organisational culture, physical and electronic security, cybercrime, military, intelligence, communication, and disaster planning and response
CLO3 : Analyse real world scenarios and apply a security engineering approach to make appropriate decisions taking into consideration key factors such as cost, human factors, risk, and privacy
CLO4 : Demonstrate and reflect upon professional competencies including analysis, time and project management, reasonableness checking, self directed research, teamwork, community building, ethical professional behaviour and effective communication
CLO5 : Apply fundamental cryptographic primitives and protocols to achieve desired properties (including confidentiality, integrity, and authentication) and explain their weaknesses and appropriate use
CLO6 : Apply concepts such as information and work measures, randomness, and privacy to design appropriate solutions for real world security problems, or recognise when no effective solutions are likely to be feasible
CLO7 : Analyse their prior approach to security in everyday life and reflect on how a security engineering mindset changes this
CLO8 : Explain the main classes of memory corruption vulnerabilities and the relative strengths and weaknesses of currently deployed countermeasures
CLO9 : Successfully attack common vulnerabilities in web based systems and binaries

Course Learning Outcomes	Assessment Item
CLO1 : Make reasonable assessments of likely future trends and emerging risks in cyber security, based on an understanding of the historical context and current developments in the field	• Portfolio • Exam
CLO2 : Demonstrate an understanding of the relationship of cyber security to related fields including safety science, psychology, organisational culture, physical and electronic security, cybercrime, military, intelligence, communication, and disaster planning and response	• Portfolio • Exam
CLO3 : Analyse real world scenarios and apply a security engineering approach to make appropriate decisions taking into consideration key factors such as cost, human factors, risk, and privacy	• Project • Portfolio • Exam
CLO4 : Demonstrate and reflect upon professional competencies including analysis, time and project management, reasonableness checking, self directed research, teamwork, community building, ethical professional behaviour and effective communication	• Project • Portfolio • Exam
CLO5 : Apply fundamental cryptographic primitives and protocols to achieve desired properties (including confidentiality, integrity, and authentication) and explain their weaknesses and appropriate use	• Portfolio • Exam
CLO6 : Apply concepts such as information and work measures, randomness, and privacy to design appropriate solutions for real world security problems, or recognise when no effective solutions are likely to be feasible	• Project • Portfolio • Exam
CLO7 : Analyse their prior approach to security in everyday life and reflect on how a security engineering mindset changes this	• Portfolio • Exam
CLO8 : Explain the main classes of memory corruption vulnerabilities and the relative strengths and weaknesses of currently deployed countermeasures	• Portfolio • Exam
CLO9 : Successfully attack common vulnerabilities in web based systems and binaries	• Portfolio • Exam

Learning and Teaching Technologies

Moodle - Learning Management System | WEB CMS course page

Learning and Teaching in this course

This course is designed to develop analytical skills and security mindset and cross-disciplinary learning on a topic of increasing importance to individuals, policymakers and businesses. The course includes additional technical cyber security material and capture the flag technical activities to introduce the main technical fields within cyber security practice. There are weekly lectures conveying fundamental concepts about security and how to apply engineering principles and design and critically analyse systems, as well as technical demonstrations and activities.

Tutorials are an opportunity to work together with peers to identify key factors in security scenarios and solve problems.

Additional Course Information

Lectures are us all together synchronously and are designed to be interactive, helpful, and to motivate you to learn. If you are enrolled in the in-person lecture stream we strongly encourage you to come along to the lectures and learn with us all together. Attendence at and participation in lectures (in person or streamed), and tutorials (in person) is compulsory and 80% attendence and participation is required to pass the course.

There is a weekly analysis case study session - probably called a "tutorial" on the online system - where you will learn in small groups analysing case studies each week and working out your own solutions to the security problems arising the the case study.

There is an optional session each week where we stay back after the lecture and watch a film and chat about it and the security concepts and behaviours it contains. It's extremely fun and entirely optional. It is probably called "seminar" in the online timetable system. One of the films will probably be used in the final exam so you should attend the movie that week or watch it yourself at home some time before the exam (we'll let you know which one in advance).

Considerable emphasis is placed on practical work, in the form of online exercises and a major self-directed project.

Students are expected to demonstrate in a sustained manner over the course that they have significant awareness and understanding of, have engaged in thoughtful reflection about, and have successfully planned to improve and develop their ability to think like an security engineer and to have mastered the course content. This is assessed by weekly online activities and a log book / portfolio.

Students in this course are welcome to (optional, not assessed) attend any or all of the classes in the associated courses if they are interested. At the time of writing there is an associated LAWS course on cyber regulation.

Students are expected to spend 150 hours on the course in total.

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
Portfolio Assessment Format: Individual	30%	
Project Assessment Format: Individual	30%	
Exam Assessment Format: Individual	40%	

Assessment Details

Portfolio

Assessment Overview

Students document and reflect on their weekly activities over the whole term.

The portfolio is marked and feedback given by the tutor.

Course Learning Outcomes

- CLO1 : Make reasonable assessments of likely future trends and emerging risks in cyber security, based on an understanding of the historical context and current developments in the field
- CLO2 : Demonstrate an understanding of the relationship of cyber security to related fields including safety science, psychology, organisational culture, physical and electronic security, cybercrime, military, intelligence, communication, and disaster planning and response
- CLO3 : Analyse real world scenarios and apply a security engineering approach to make appropriate decisions taking into consideration key factors such as cost, human factors, risk, and privacy
- CLO4 : Demonstrate and reflect upon professional competencies including analysis, time and project management, reasonableness checking, self directed research, teamwork, community building, ethical professional behaviour and effective communication
- CLO5 : Apply fundamental cryptographic primitives and protocols to achieve desired properties (including confidentiality, integrity, and authentication) and explain their weaknesses and appropriate use
- CLO6 : Apply concepts such as information and work measures, randomness, and privacy to design appropriate solutions for real world security problems, or recognise when no effective solutions are likely to be feasible
- CLO7 : Analyse their prior approach to security in everyday life and reflect on how a security engineering mindset changes this
- CLO8 : Explain the main classes of memory corruption vulnerabilities and the relative strengths and weaknesses of currently deployed countermeasures

- CLO9 : Successfully attack common vulnerabilities in web based systems and binaries

Detailed Assessment Description

30% - Mark from tutors, based on weekly engagement in tutorials and weekly completion of relevant online activities. Mark is based on 'best' 7 weeks.

Assessment Length

N/A

Submission notes

Varied

Assessment information

Except in extremely exceptional circumstances, there is no special consideration for this assessment. Students are assessed on the basis of the 'best' 7 weeks of submissions. Students are expected to submit *every* week except where a substantial and extended unforeseen circumstance occurs. Such unforeseen circumstances should thus not affect the students' grade unless the substantial unforeseen circumstance prevents submission three or more times.

Assignment submission Turnitin type

This is not a Turnitin assignment

Generative AI Permission Level

Simple Editing Assistance

In completing this assessment, you are permitted to use standard editing and referencing functions in the software you use to complete your assessment. These functions are described below. You must not use any functions that generate or paraphrase passages of text or other media, whether based on your own work or not.
If your Convenor has concerns that your submission contains passages of AI-generated text or media, you may be asked to account for your work. If you are unable to satisfactorily demonstrate your understanding of your submission you may be referred to UNSW Conduct & Integrity Office for investigation for academic misconduct and possible penalties.
For more information on Generative AI and permitted use please see here.

Students are permitted to use translation, spell-check, and grammar correction tools only.

Project

Assessment Overview

Students work on a project of their choice. The project must be approved by the tutor, who also marks the project report and provides feedback.

The project work is also presented in a tutorial, with feedback from the other students.

Course Learning Outcomes

- CLO3 : Analyse real world scenarios and apply a security engineering approach to make appropriate decisions taking into consideration key factors such as cost, human factors, risk, and privacy
- CLO4 : Demonstrate and reflect upon professional competencies including analysis, time and project management, reasonableness checking, self directed research, teamwork, community building, ethical professional behaviour and effective communication
- CLO6 : Apply concepts such as information and work measures, randomness, and privacy to design appropriate solutions for real world security problems, or recognise when no effective solutions are likely to be feasible

Detailed Assessment Description

This will be discussed in detail with students in the course. Students choose a project that will challenge them and develop a plan to complete the project the course over the semester.

Assessment Length

N/A

Submission notes

Moodle

Assessment information

N/A

Assignment submission Turnitin type

This is not a Turnitin assignment

Generative AI Permission Level

Simple Editing Assistance

In completing this assessment, you are permitted to use standard editing and referencing functions in the software you use to complete your assessment. These functions are described below. You must not use any functions that generate or paraphrase passages of text or other

media, whether based on your own work or not.
If your Convenor has concerns that your submission contains passages of AI-generated text or media, you may be asked to account for your work. If you are unable to satisfactorily demonstrate your understanding of your submission you may be referred to UNSW Conduct & Integrity Office for investigation for academic misconduct and possible penalties.
For more information on Generative AI and permitted use please see here.

Some students' projects may use generative AI *as part of the project itself*. In that case, the use of generative AI should be disclosed in the proposal. Otherwise, students are permitted to use translation, spell-check, and grammar correction tools only.

Exam

Assessment Overview

A take home exam in the UNSW exam period, covering all topics in the course. Marked by the lecturer and tutors.

Course Learning Outcomes

- CLO1 : Make reasonable assessments of likely future trends and emerging risks in cyber security, based on an understanding of the historical context and current developments in the field
- CLO2 : Demonstrate an understanding of the relationship of cyber security to related fields including safety science, psychology, organisational culture, physical and electronic security, cybercrime, military, intelligence, communication, and disaster planning and response
- CLO3 : Analyse real world scenarios and apply a security engineering approach to make appropriate decisions taking into consideration key factors such as cost, human factors, risk, and privacy
- CLO4 : Demonstrate and reflect upon professional competencies including analysis, time and project management, reasonableness checking, self directed research, teamwork, community building, ethical professional behaviour and effective communication
- CLO5 : Apply fundamental cryptographic primitives and protocols to achieve desired properties (including confidentiality, integrity, and authentication) and explain their weaknesses and appropriate use
- CLO6 : Apply concepts such as information and work measures, randomness, and privacy to design appropriate solutions for real world security problems, or recognise when no effective solutions are likely to be feasible
- CLO7 : Analyse their prior approach to security in everyday life and reflect on how a security engineering mindset changes this
- CLO8 : Explain the main classes of memory corruption vulnerabilities and the relative strengths and weaknesses of currently deployed countermeasures
- CLO9 : Successfully attack common vulnerabilities in web based systems and binaries

Detailed Assessment Description

Take home exam

Open book

Assessment Length

2 hours done over 3 hours

Submission notes

Typed and submitted online

Assignment submission Turnitin type

This is not a Turnitin assignment

Generative AI Permission Level

No Assistance

This assessment is designed for you to complete without the use of any generative AI. You are not permitted to use any generative AI tools, software or service to search for or generate information or answers.
For more information on Generative AI and permitted use please see here.

General Assessment Information

Grading Basis

Standard

Requirements to pass course

A final mark over 50% and 80% attendance+participation in tutorials and lectures.

Course Schedule

Attendance Requirements

Students must attend+participate in 80% of lectures and 80% of tutorials, as a requirement to pass the course.

Please be advised there will be no classes on public holidays. If your class falls on a public holiday, alternative arrangements will be made by the course convenor to make up the missed class.

General Schedule Information

Monday lecture (enrol in synchronous online version if that is your intent) 6-8pm

Tuesday lecture (enrol in synchronous online version if that is your intent) 4-6pm

Thursday lecture (enrol in synchronous online version if that is your intent) 6-8pm

Tutorial (timing varies)

OPTIONAL ACTIVITIES:

Tuesday "Security Theatre" movie night 6-8pm

Course Resources

Prescribed Resources

Online materials

Recommended Resources

Online materials, and information in classes and tutorials.

Additional Costs

None. There will be one mandatory movie viewing, we will show for free, but students unable to attend that session may need to rent it from a streaming provider.

Course Evaluation and Development

The main suggestions for change from the last time this course was taught (and our responses for this time) are:

1. Complexity of submission of weekly reflections and greater flexibility. Going forward, students will only need to submit (1) heading, (2) link (or the answer itself), and (3) asterisk next to best activity of the week. Further only the 'best' 7 weeks will count towards the student's grade.

2. Explaining the point of the weekly activities to students at the outset. Will allow some time in the first lecture and tutorial to discuss our intentions behind the course design rather than leaving it to the las lecture as we previously did. Also more explanation on each activity type.

3. Inconsistent communications (tutors, Richard, Kris, Lyria, etc). Centralise communication around assessment and course structure - class Q & A forum.

4. Clearer and elaboration of assessment requirements (eg rubrics). Will be done, plus opportunity to ask questions on the central Q&A forum.

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Head lecturer	Richard Buckland				will stay back after lectures for as long as needed to answer any questions	Yes	Yes
Administrator	Caitlin O'Brien				email class email address to reach the class admin team and lecturers, if a confidential email is needed email Caitlin at her personal address caitlin.obrien@unsw.edu.au	No	No
Lecturer	Kristian Mansfield				will stay back after lectures for as long as needed to answer any questions	No	No

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 Contact Information

CSE Help! - on the Ground Floor of K17

- For assistance with coursework assessments.

The Nucleus Student Hub - https://nucleus.unsw.edu.au/en/contact-us

- Course enrolment queries.

Grievance Officer - grievance-officer@cse.unsw.edu.au

- If the course convenor gives an inadequate response to a query or when the courses convenor does not respond to a query about assessment.

Student Reps - stureps@cse.unsw.edu.au

- If some aspect of a course needs urgent improvement. (e.g. Nobody responding to forum queries, cannot understand the lecturer)

You should **never** contact any of the following people directly:

- Vice Chancellor

- Pro-vice Chancellor Education (PVCE)

- Head of School

- CSE administrative staff

- CSE teaching support staff

They will simply bounce the email to one of the above, thereby creating an unnecessary level of indirection and a delay in the response.