UNSW Course Outline

ZEIT3120 Programming for Security - 2024

Published on the 09 Feb 2024

General Course Information

Course Code : ZEIT3120
Year : 2024
Term : Semester 1
Teaching Period : Z1
Is a multi-term course? : No
Faculty : UNSW Canberra
Academic Unit : School of Systems and Computing
Delivery Mode : In Person
Delivery Format : Standard
Delivery Location : UNSW Canberra at ADFA
Campus : UNSW Canberra
Study Level : Undergraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

Students will learn how to assess their code and software stack for vulnerabilities additionally they will discover how those vulnerabilities are exploited, and how to mitigate those vulnerabilities. Historical and current approaches to exploitation and defence will be explored.

Students will gain a deep understanding of software vulnerabilities through hands on experience.

Topics covered will include: input validation, data security, cryptography, hashes, random numbers, anti-tampering, fuzzing, overflow, and Return-oriented programming.

Course Aims

This course equips the student to understand and include cryptography in applications and enable the student to develop secure Java applications using standard protocols such as SSL and S/ MIME

Course Learning Outcomes

Course Learning Outcomes
CLO1 : Demonstrate an understanding of symmetric encryption, asymmetric encryption , and integrity checking.
CLO2 : Demonstrate an understanding of creating and using secured channels using SSL.
CLO3 : Given a system, be able to identify vulnerabilities and exploit them.
CLO4 : Given a system, be able to identify vulnerabilities and design and implement reliable countermeasures to prevent successful exploitation.

Course Learning Outcomes	Assessment Item
CLO1 : Demonstrate an understanding of symmetric encryption, asymmetric encryption , and integrity checking.	• Tutorial Test • Assignment 1 • Assignment 2
CLO2 : Demonstrate an understanding of creating and using secured channels using SSL.	• Tutorial Test • Assignment 1 • Assignment 2
CLO3 : Given a system, be able to identify vulnerabilities and exploit them.	• CTF • Assignment 2
CLO4 : Given a system, be able to identify vulnerabilities and design and implement reliable countermeasures to prevent successful exploitation.	• CTF • Assignment 2

Learning and Teaching Technologies

Moodle - Learning Management System | Echo 360

Learning and Teaching in this course

All information about the course can be found on the course website on Moodle.

In addition, the following references will be used and are optional.

Additional Course Information

Students will learn how to use cryptography in their software applications and understand how cryptography is being used. Knowledge of object oriented programming is necessary, but students need not be familiar with any of the APIs discussed or any particular programming language. Students will be able to use C, C++, Java, or Python to complete their assignments and coursework. This course is hands-on and includes programming assignments, scripting work and capture the flag (CTF) type problems. This course aims to encourage students to build skills designing, developing prototypes, evaluating, and critiquing systems. Students will develop the skills required to integrate cryptography into developing secure software systems. Additionally, Students will learn how to identify potential vulnerabilities in their applications and how vulnerabilities are exploited.

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
Tutorial Test Assessment Format: Individual	10%	Start Date: Not Applicable Due Date: Week 3: 11 March - 15 March
Assignment 1 Assessment Format: Individual	30%	Start Date: 03/04/2024 06:00 PM Due Date: 03/05/2024 06:00 PM
CTF Assessment Format: Individual	30%	Start Date: Not Applicable Due Date: Not Applicable
Assignment 2 Assessment Format: Individual	30%	Start Date: 17/04/2024 06:00 PM Due Date: 17/06/2024 06:00 PM

Assessment Details

Tutorial Test

Course Learning Outcomes

- CLO1 : Demonstrate an understanding of symmetric encryption, asymmetric encryption , and integrity checking.
- CLO2 : Demonstrate an understanding of creating and using secured channels using SSL.

Detailed Assessment Description

This is a formative assessment that will allow students to demonstrate and develop their understanding of the concepts in topic areas covered in the course.

Assessment Length

1 hour

Submission notes

This will be in your tutorial time

Assignment 1

Course Learning Outcomes

- CLO1 : Demonstrate an understanding of symmetric encryption, asymmetric encryption , and integrity checking.
- CLO2 : Demonstrate an understanding of creating and using secured channels using SSL.

Detailed Assessment Description

This is a written and programming task that will examine and develop the students knowledge of the cryptography section of the course

Submission notes

Sumission via moodle

Assignment submission Turnitin type

Not Applicable

CTF

Course Learning Outcomes

- CLO3 : Given a system, be able to identify vulnerabilities and exploit them.
- CLO4 : Given a system, be able to identify vulnerabilities and design and implement reliable countermeasures to prevent successful exploitation.

Detailed Assessment Description

Capture the flag style tasks will be given to students throughout the course, students are expected to work on and solve these tasks individually during their Labs. Their tutor will assess their completion during lab time.

Assignment 2

Course Learning Outcomes

- CLO1 : Demonstrate an understanding of symmetric encryption, asymmetric encryption , and integrity checking.
- CLO2 : Demonstrate an understanding of creating and using secured channels using SSL.
- CLO3 : Given a system, be able to identify vulnerabilities and exploit them.

- CLO4 : Given a system, be able to identify vulnerabilities and design and implement reliable countermeasures to prevent successful exploitation.

Detailed Assessment Description

Assignment 2 will provide an opportunity for students to demonstrate their skills in solving a more complex problem and coding a solution. This assignment will be a group work assignment.

Submission notes

Submit the writtern component via Moodle

Assessment information

Assignment 2 presentations - will be in class time at both the lab and lecture during week 13

Assignment submission Turnitin type

Not Applicable

General Assessment Information

Grading Basis

Standard

Requirements to pass course

To qualify for a passing grade all CTFs must be satisfactorily completed.

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 1 : 26 February - 1 March	Topic	Overview - locks and doors
Week 2 : 4 March - 8 March	Topic	Entropy / encryption / compression and Historical encryption techniques Message Digests, MACc and HMACs and Modern Symmetric encryption
Week 3 : 11 March - 15 March	Topic	Canberra day - No Lecture this week
	Assessment	In class test, will occur in lab time
Week 4 : 18 March - 22 March	Topic	Asymmetric encryption
Week 5 : 25 March - 29 March	Topic	Permissions, selinux and Apparmor and Known current and historical attacks
Week 6 : 1 April - 5 April	Topic	No Class this week. Easter monday
Week 7 : 22 April - 26 April	Topic	Securing data - stationary No lab on the 24th due to millitary training day
Week 8 : 29 April - 3 May	Topic	Dealing with user input
	Assessment	Assignment 1 due by 6pm on the 3rd of May
Week 9 : 6 May - 10 May	Topic	SSL & TLS
Week 10 : 13 May - 17 May	Topic	ASLR, stack canaries, and other tools
Week 11 : 20 May - 24 May	Topic	Basic disassembly and debugging
Week 12 : 27 May - 31 May	Topic	Fuzzing and Shared libraries the good and evil
Week 13 : 3 June - 7 June	Topic	Assignment 2 presentations - these will be in class time at both the lab and lecture
	Assessment	Written component of assignment 2 due Jun 17th 6pm.

Attendance Requirements

Students are strongly encouraged to attend all classes and review lecture recordings. Lecture recordings may not always be possible. CTFs will be dononstrated and evaluated in the lab during the lab.

Course Resources

Prescribed Resources

There is no compulsory text for this course. There are just recommended readings.

Recommended Resources

Viega, J., & Messier, M. (2003). Secure Programming Cookbook for C and C++: Recipes for Cryptography, Authentication, Input Validation & More. New York.

Course Evaluation and Development

One of the key priorities in the 2025 Strategy for UNSW is a drive for academic excellence in education. One of the ways of determining how well UNSW is progressing towards this goal is by listening to our own students. Students will be asked to complete the myExperience survey towards the end of this course.

Students can also provide feedback during the semester via: direct contact with the lecturer, the “On-going Student Feedback” link in Moodle, Student-Staff Liaison Committee meetings in schools, informal feedback conducted by staff, and focus groups. Student opinions really do make a difference. Refer to the Moodle site for this course to see how the feedback from previous students has contributed to the course development.

Important note: Students are reminded that any feedback provided should be constructive and professional and that they are bound by the Student Code of Conduct Policy

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Convenor	Tim Lynar		Building 15 room 114	02 5114 5175	by appointment,	Yes	Yes

Other Useful Information

Academic Information

Course Evaluation and Development

One of the key priorities in the 2025 Strategy for UNSW is a drive for academic excellence in education. One of the ways of determining how well UNSW is progressing towards this goal is by listening to our own students. Students will be asked to complete the myExperience survey towards the end of each course.

Students can also provide feedback during the semester via: direct contact with the lecturer, the "On-going Student Feedback" link in Moodle, Student-Staff Liaison Committee meetings in schools, informal feedback conducted by staff, and focus groups (where applicable). Student opinions really do make a difference. Refer to the Moodle site for your course to see how the feedback from previous students has contributed to the course development.

Important note: Students are reminded that any feedback provided should be constructive and professional and that they are bound by the Student Code of Conduct.

https://www.gs.unsw.edu.au/policy/documents/studentcodepolicy.pdf

Equitable Learning Services (ELS)

Students living with neurodivergent, physical and/or mental health conditions or caring for someone with these conditions may be eligible for support through the Equitible Learning Services team. Equitable Learning Services is a free and confidential service that provides practical support to ensure your mental or physical health conditions do not adversely affect your studies.

Our team of dedicated **Equitable Learning Facilitators** (ELFs) are here to assist you through this process. We offer a number of services to make your education at UNSW easier and more equitable.

Further information about ELS for currently enrolled students can be found at: https://www.student.unsw.edu.au/equitable-learning

Academic Honesty and Plagarism

UNSW has an ongoing commitment to fostering a culture of learning informed by academic integrity. All UNSW staff and students have a responsibility to adhere to this principle of academic integrity. All students are expected to adhere to UNSW's Student Code of Conduct. Find relevant information at: Student Code of Conduct (unsw.edu.au)

Plagiarism undermines academic integrity and is not tolerated at UNSW. It is defined as using the words or ideas of others and passing them off as your own, and can take many forms, from deliberate cheating to accidental copying from a source without acknowledgement.

For more information, please refer to the following:

https://student.unsw.edu.au/plagiarism

Submission of Assessment Tasks

Special Consideration

Special Consideration is the process for assessing and addressing the impact on students of short-term events, that are beyond the control of the student, and that affect performance in a specific assessment task or tasks.

Applications for Special Consideration will be accepted in the following circumstances only:

- Where academic work has been hampered to a substantial degree by illness or other cause;
- The circumstances are unexpected and beyond the student's control;
- The circumstances could not have reasonably been anticipated, avoided or guarded against by the student; and either:

(i) they occurred during a critical study period and was 3 consecutive days or more duration, or a total of 5 days within the critical study period; or

(ii) they prevented the ability to complete, attend or submit an assessment task for a specific date (e.g. final exam, in class test/quiz, in class presentation)

Applications for Special Consideration must be made as soon as practicable after the problem occurs and at the latest within three working days of the assessment or the period covered by the supporting documentation.

By sitting or submitting the assessment task the student is declaring that they are fit to do so and cannot later apply for Special Consideration (UNSW 'fit to sit or submit' requirement).

Sitting, accessing or submitting an assessment task on the scheduled assessment date, after applying for special consideration, renders the special consideration application void.

Find more information about special consideration at: https://www.student.unsw.edu.au/special/consideration/guide

Or apply for special consideration through your MyUNSW portal.

Late Submission of assessment tasks (other than examinations)

UNSW has a standard late submission penalty of:

- 5% per day,
- capped at five days (120 hours) from the assessment deadline, after which a student cannot submit an assessment, and
- no permitted variation.

Students are expected to manage their time to meet deadlines and to request extensions as early as possible before the deadline.

Electronic submission of assessment

Except where the nature of an assessment task precludes its electronic submission, all assessments must be submitted to an electronic repository, approved by UNSW or the Faculty, for archiving and subsequent marking and analysis.

Release of final mark

All marks obtained for assessment items during the session are provisional. The final mark as published by the university following the assessment review group meeting is the only official mark.

School-specific Information

The Leaning Management System

Moodle is the Learning Management System used at UNSW Canberra. All courses have a Moodle site which will become available to students at least one week before the start of semester.

Please find all help and documentation (including Blackboard Collaborate) at the Moodle Support page.

UNSW Moodle supports the following web browsers:
• Google Chrome 50+
• Safari 10+
Internet Explorer is not recommended. Addons and Toolbars can affect any browser's performance.

Operating systems recommended are:
• Windows 10,
• Mac OSX Sierra,
• iPad IOS10

Further details:
Moodle System Requirements
Moodle Log In

If you need further assistance with Moodle:

For enrolment and login issues please contact:
IT Service Centre
Email: itservicecentre@unsw.edu.au
Phone: (02) 9385-1333
International: +61 2 9385 1333

For all other Moodle issues please contact:
External TELT Support
Email: externalteltsupport@unsw.edu.au
Phone: (02) 9385-3331
International: +61 2 938 53331
Opening hours:
Monday – Friday 7:30am – 9:30 pm
Saturday & Sunday 8:30 am – 4:30pm

Study at UNSW Canberra
Study at UNSW Canberra has lots of useful information regarding:
• Where to get help

• Administrative matters
• Getting your passwords set up
• How to log on to Moodle
• Accessing the Library and other areas.

UNSW Canberra Student Hub

For News and Notices, Student Services and Support, Campus Comminity, Quick Links, Important Dates and Upcoming Events

School Contact Information

Deputy Head of School (Education): Dr Erandi Hene Kankanamge
E: e.henekankanamge@adfa.edu.au
T: 02 5114 5157

Syscom Admin Support: syscom@unsw.edu.au
T: 02 5114 5284
Syscom Admin Office: Building 15, Level 1, Room 101 (open 10am to 3pm, Mon to Fri)