UNSW Course Outline

ZEIT8024 Software Security Lifecycle - 2024

Published on the 09 Feb 2024

General Course Information

Course Code : ZEIT8024
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 : Online
Delivery Format : Standard
Delivery Location : UNSW Canberra at ADFA
Campus : UNSW Canberra
Study Level : Postgraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

The world is more digitally connected than it has ever been before with the digitisation of money and content, supporting e-commerce and access from anywhere via fixed or mobile networks. The integrity of such critical digital assets then depends on the reliability and security of the

software that enables and controls those assets. According to the latest reports, software application vulnerabilities are ranked the No.1 threat to information security professionals and will continue to be among the top cyber security concerns.

While attackers and researchers continue to expose new application vulnerabilities, the many common application flaws are very often previous, rediscovered threats. In many cases software applications operate as part of a larger systems thus face a number of different security risks. For example, security issues associated with implementing COTS software within existing systems. Most importantly, developing web applications in this current environment requires an understanding of:

- all security issues associated with software components and their interfaces within the larger system; and
- applicability of a holistic approach to ***build security in*** starting from a user requirements, software design and implementation to testing and deployment.

This Masterscourse is designed to provide students with a deep understanding, and the skills to implement, manage and incorporate security practices throughout the whole Software Development Lifecycle (SDLC), from identifying customer needs, writing secure requirements, designing, implementing, testing and deployment.

This course meets an essential requirement for software developers to stay current on the latest advances in software development and the new security threats they create. This course is theoretical and covers not only the content of the ISC2 CSSLP® certification, but also provides a holistic view on a role of software applications within complex systems. It draws on ISC2 material as well as other scholarly sources.

Topics include:

- Secure Software Concepts
- Secure Software Requirements
- Secure Software Design
- Secure Software Implementation / Coding
- Secure Software Testing
- Software Acceptance
- Software Deployment Operations, Maintenance and Disposal

Course Aims

This course aims to:provide students with a deep understanding of, and the ability to implement and manage, security throughout the software development lifecycle.

Course Learning Outcomes

Course Learning Outcomes
CLO1 : On completion of this course, students should be able to: understand the relationship between software development and secure software development approaches, practices and frameworks, the relevance and need for ensuring software is secure and the implications of this throughout all the phases of a development lifecycle.
CLO2 : On completion of this course, students should be able to: investigate the need and strategies for identifying and evaluating security requirements and the practical implementation of embedding these as part the development lifecycle.
CLO3 : On completion of this course, students should be able to: explain different types of testing for security functionality and resiliency to cyber-attacks.
CLO4 : On completion of this course, students should be able to: demonstrate an understanding of security best practices within software application development lifecycles.
CLO5 : On completion of this course, students should be able to: investigate, understand and demonstrate current practices and modern and evolving approaches to secure software.

Course Learning Outcomes	Assessment Item
CLO1 : On completion of this course, students should be able to: understand the relationship between software development and secure software development approaches, practices and frameworks, the relevance and need for ensuring software is secure and the implications of this throughout all the phases of a development lifecycle.	• Case Study • Integration Model • Research Report
CLO2 : On completion of this course, students should be able to: investigate the need and strategies for identifying and evaluating security requirements and the practical implementation of embedding these as part the development lifecycle.	• Case Study • Integration Model • Research Report
CLO3 : On completion of this course, students should be able to: explain different types of testing for security functionality and resiliency to cyber-attacks.	• Online Quiz • Integration Model • Research Report
CLO4 : On completion of this course, students should be able to: demonstrate an understanding of security best practices within software application development lifecycles.	• Online Quiz • Integration Model • Research Report
CLO5 : On completion of this course, students should be able to: investigate, understand and demonstrate current practices and modern and evolving approaches to secure software.	• Case Study • Online Quiz • Research Report

Learning and Teaching Technologies

Moodle - Learning Management System

Learning and Teaching in this course

There is no prescribed textbook that students need to acquire. A variety of resource materials will be made available.

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
Case Study Assessment Format: Individual	15%	Start Date: 01/03/2024 12:00 AM Due Date: 15/03/2024 08:00 PM
Integration Model Assessment Format: Individual	20%	Start Date: 20/03/2024 08:00 PM Due Date: 17/04/2024 08:00 PM
Research Report Assessment Format: Individual	40%	Start Date: 17/04/2024 08:00 PM Due Date: 29/05/2024 08:00 PM
Practical Exercise Participation Assessment Format: Individual	10%	Start Date: Not Applicable Due Date: Not Applicable
Online Quiz Assessment Format: Individual	15%	Start Date: 29/05/2024 08:00 PM Due Date: 05/06/2024 08:00 PM

Assessment Details

Case Study

Assessment Overview

A case study focussing on software vulnerabilities today. Students will need to provide a report in the form of a short executive summary presentation in PowerPoint format focussing on relevant points only.

Course Learning Outcomes

- CLO1 : On completion of this course, students should be able to: understand the relationship between software development and secure software development approaches, practices and frameworks, the relevance and need for ensuring software is secure and the implications of this throughout all the phases of a development lifecycle.
- CLO2 : On completion of this course, students should be able to: investigate the need and strategies for identifying and evaluating security requirements and the practical implementation of embedding these as part the development lifecycle.
- CLO5 : On completion of this course, students should be able to: investigate, understand and demonstrate current practices and modern and evolving approaches to secure software.

Detailed Assessment Description

A Case Study focussing on software vulnerabilities today. Students will need to provide a report in the form of a short executive summary presentation in PowerPoint format focussing on relevant points only

Assignment submission Turnitin type

Not Applicable

Integration Model

Assessment Overview

This assessment will require students to investigate a specific form of software development and provide both an analysis of this and a suggested secure software integration model.

Course Learning Outcomes

- CLO1 : On completion of this course, students should be able to: understand the relationship between software development and secure software development approaches, practices and frameworks, the relevance and need for ensuring software is secure and the implications of this throughout all the phases of a development lifecycle.
- CLO2 : On completion of this course, students should be able to: investigate the need and strategies for identifying and evaluating security requirements and the practical implementation of embedding these as part the development lifecycle.
- CLO3 : On completion of this course, students should be able to: explain different types of testing for security functionality and resiliency to cyber-attacks.
- CLO4 : On completion of this course, students should be able to: demonstrate an understanding of security best practices within software application development lifecycles.

Detailed Assessment Description

This assessment will require students to investigate a specific form of software development and provide both an analysis of this and a suggested secure software integration model.

Assignment submission Turnitin type

Not Applicable

Research Report

Assessment Overview

This will require students to engage in significant comparative research into, and analysis of, current organisational implementations of secure software development and make a realistic assessment of these in terms of a set of recommended practices relating to a given scenario.

Course Learning Outcomes

- CLO1 : On completion of this course, students should be able to: understand the relationship between software development and secure software development approaches, practices and frameworks, the relevance and need for ensuring software is secure and the implications of this throughout all the phases of a development lifecycle.
- CLO2 : On completion of this course, students should be able to: investigate the need and strategies for identifying and evaluating security requirements and the practical implementation of embedding these as part the development lifecycle.
- CLO3 : On completion of this course, students should be able to: explain different types of testing for security functionality and resiliency to cyber-attacks.
- CLO4 : On completion of this course, students should be able to: demonstrate an understanding of security best practices within software application development lifecycles.
- CLO5 : On completion of this course, students should be able to: investigate, understand and demonstrate current practices and modern and evolving approaches to secure software.

Detailed Assessment Description

This will require students to engage in significant comparative research into, and analysis of, current organisational implementations of secure software development and make a realistic assessment of these in terms of a set of recommended practices relating to given scenario.

Assignment submission Turnitin type

Not Applicable

Practical Exercise Participation

Assessment Overview

While practical exercises will not be assessed, participation and effort will be monitored and marks awarded accordingly.

Detailed Assessment Description

While practical exercises will not be assessed, participation and effort will be monitored and marks awarded accordingly

Assessment information

While practical exercises will not be assessed, participation and effort will be monitored and marks awarded accordingly.

Assignment submission Turnitin type

Not Applicable

Online Quiz

Assessment Overview

This is a 30 question open-book Online Quiz. The quiz will be available for a week during which students will have one attempt to complete at a time they choose.

Course Learning Outcomes

- CLO3 : On completion of this course, students should be able to: explain different types of testing for security functionality and resiliency to cyber-attacks.
- CLO4 : On completion of this course, students should be able to: demonstrate an understanding of security best practices within software application development lifecycles.
- CLO5 : On completion of this course, students should be able to: investigate, understand and demonstrate current practices and modern and evolving approaches to secure software.

Detailed Assessment Description

This is an 30 question open-book Online Quiz. The quiz will be available for a week during which students will have one attempt to complete at a time they choose.

Assignment submission Turnitin type

Not Applicable

General Assessment Information

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.**

Grading Basis

Standard

Requirements to pass course

To pass this subject, students will need to achieve at least 50 marks out of a total 100 marks overall.

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 1 : 26 February - 1 March	Topic	Mod 1 Introduction - Cybersecurity Concepts Why Secure Software? Software Development and Security – History, Fundamentals and Principals
Week 2 : 4 March - 8 March	Topic	Mod 2 Modern Software Development Frameworks – (Waterfall to Agile)
Week 3 : 11 March - 15 March	Topic	Mod 3 Overview of Scrum
Week 4 : 18 March - 22 March	Topic	Mod 4 Secure Software Frameworks and Practices
Week 5 : 25 March - 29 March	Topic	Mod 5 Understanding Cyberattacks and Malware
Week 6 : 1 April - 5 April	Topic	Mod 6 Vulnerability and Risk Assessment and Threat Modelling
Week 7 : 22 April - 26 April	Topic	Mod 7 Security Requirements Security in Architecture and Design
Week 8 : 29 April - 3 May	Topic	Mod 8 Implementation – Coding and Secure Practices
Week 9 : 6 May - 10 May	Topic	Mod 9 Testing for Security Test Automation
Week 10 : 13 May - 17 May	Topic	Mod 10 Acceptance/delivery, Deployment, Operations Maintenance and Disposal
Week 11 : 20 May - 24 May	Topic	Mod 11 Software Development Today - Continuous Delivery - DevOps and DevSecOps
Week 12 : 27 May - 31 May	Topic	Mod 12 CI/CD, Toolchains and Pipelines
Week 13 : 3 June - 7 June	Topic	Mod 13 Modern Secure Software Development in Practice - a Case Study Course Summary and Conclusion

Attendance Requirements

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

Course Resources

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

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

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Convenor	Timothy Lynar		15/114	+61 2 5114 5175	by appointment	No	No
Lecturer	Brian Farnhill		Consultation via Teams, Moodle Collaborate or Zoom		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)