UNSW Course Outline

ZINT2100 Introduction to Cyber-Security: Policy & Operations - 2024

Published on the 09 Feb 2024

General Course Information

Course Code : ZINT2100
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

Cyber-security is headline news and a growing challenge for national and global security, while computer technology now pervades every aspect of the personal and professional lives of our graduates. This technology underpins enormous performance improvements but also brings serious vulnerabilities. The many forms of cyber-threats - such as data theft, surveillance, and system compromise - have become tools of activism, corporate and state espionage, warfare, counter-proliferation, and intelligence gathering. This course provides an in-depth introduction to the strategic and national security challenges of cybersecurity, and provides students with the skills to defend their organisation and their personal computers from the most common forms of attack.

Course Aims

This course provides an in-depth introduction to the strategic and national security challenges of cybersecurity, and provides students with the skills to defend their organisation and their personal computers from the most common forms of attack.

Course Learning Outcomes

Course Learning Outcomes
CLO1 : Develop a practical understanding of the organisational, policy and national security contexts in which cybersecurity is important
CLO2 : Understand the historical context cybersecurity draws on
CLO3 : Evaluate the evolving legal and normative context in which cybersecurity is being discussed internationally
CLO4 : Analyse specific cases in which cybersecurity vulnerabilities and conflicts are occurring
CLO5 : Describe the common attack methodologies and relevant defence approaches of cyber security
CLO6 : Outline an effective defence-in-depth cyber environment for an organisation
CLO7 : Evaluate cyber defence capabilities of personal computing facilities
CLO8 : Practice appropriate levels of security in personal computing

Course Learning Outcomes	Assessment Item
CLO1 : Develop a practical understanding of the organisational, policy and national security contexts in which cybersecurity is important	• Cybersecurity Brief – Part 1 • Final Exam
CLO2 : Understand the historical context cybersecurity draws on	• Cybersecurity Brief – Part 1 • Final Exam
CLO3 : Evaluate the evolving legal and normative context in which cybersecurity is being discussed internationally	• Cybersecurity Brief – Part 1 • Final Exam
CLO4 : Analyse specific cases in which cybersecurity vulnerabilities and conflicts are occurring	• Cybersecurity Brief – Part 2 • Cybersecurity Brief – Part 3 • Final Exam
CLO5 : Describe the common attack methodologies and relevant defence approaches of cyber security	• Cybersecurity Brief – Part 2 • Cybersecurity Brief – Part 3 • Final Exam
CLO6 : Outline an effective defence-in-depth cyber environment for an organisation	• Cybersecurity Brief – Part 2 • Cybersecurity Brief – Part 3 • Final Exam
CLO7 : Evaluate cyber defence capabilities of personal computing facilities	• Lab • Final Exam
CLO8 : Practice appropriate levels of security in personal computing	• Lab • Final Exam

Learning and Teaching Technologies

Moodle - Learning Management System

Learning and Teaching in this course

There is no compulsory text for this course. There are compulsory and recommended readings. These are available on the course Moodle page. Compulsory readings set MUST be completed prior to the lecture, and knowledge from them will be used as a basis for the exam.

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
Cybersecurity Brief – Part 1 Assessment Format: Group	10%	Start Date: 28/02/2024 10:00 AM Due Date: 15/03/2024 11:55 PM
Cybersecurity Brief – Part 2 Assessment Format: Individual	15%	Start Date: 04/04/2024 10:00 AM Due Date: 03/05/2024 11:55 PM
Lab Assessment Format: Group	20%	Start Date: 30/04/2024 01:00 PM Due Date: 17/05/2024 11:55 PM
Cybersecurity Brief – Part 3 Assessment Format: Individual	15%	Start Date: 07/05/2024 12:00 PM Due Date: 17/05/2024 11:55 PM
Final Exam Assessment Format: Individual	40%	

Assessment Details

Cybersecurity Brief – Part 1

Assessment Overview

Identify a cybersecurity challenge and related organisation responsibilities

Course Learning Outcomes

- CLO1 : Develop a practical understanding of the organisational, policy and national security contexts in which cybersecurity is important
- CLO2 : Understand the historical context cybersecurity draws on
- CLO3 : Evaluate the evolving legal and normative context in which cybersecurity is being discussed internationally

Cybersecurity Brief – Part 2

Assessment Overview

Risk assessment and mitigation strategy against certain vulnerabilities.

Course Learning Outcomes

- CLO4 : Analyse specific cases in which cybersecurity vulnerabilities and conflicts are occurring

- CLO5 : Describe the common attack methodologies and relevant defence approaches of cyber security
- CLO6 : Outline an effective defence-in-depth cyber environment for an organisation

Lab

Assessment Overview

Group work in which students will evaluate and then later configure the cyber-security capabilities of virtual machines.

Course Learning Outcomes

- CLO7 : Evaluate cyber defence capabilities of personal computing facilities
- CLO8 : Practice appropriate levels of security in personal computing

Submission notes

Students who have labs on Friday will submit their lab reports on 24th May due to Military training day.

Cybersecurity Brief – Part 3

Assessment Overview

Residual Risk of work, key recommendations.

Course Learning Outcomes

- CLO4 : Analyse specific cases in which cybersecurity vulnerabilities and conflicts are occurring
- CLO5 : Describe the common attack methodologies and relevant defence approaches of cyber security
- CLO6 : Outline an effective defence-in-depth cyber environment for an organisation

Final Exam

Course Learning Outcomes

- CLO1 : Develop a practical understanding of the organisational, policy and national security contexts in which cybersecurity is important
- CLO2 : Understand the historical context cybersecurity draws on
- CLO3 : Evaluate the evolving legal and normative context in which cybersecurity is being discussed internationally
- CLO4 : Analyse specific cases in which cybersecurity vulnerabilities and conflicts are occurring
- CLO5 : Describe the common attack methodologies and relevant defence approaches of cyber security
- CLO6 : Outline an effective defence-in-depth cyber environment for an organisation
- CLO7 : Evaluate cyber defence capabilities of personal computing facilities

- CLO8 : Practice appropriate levels of security in personal computing

General Assessment Information

Grading Basis

Standard

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 1 : 26 February - 1 March	Lecture	Introducing the Concepts and history of Cybersecurity
	Tutorial	
Week 2 : 4 March - 8 March	Lecture	The Cyber Problem and Domestic Issues
	Tut-Lab	
Week 3 : 11 March - 15 March	Lecture	Ethics of Cyber Security
	Tutorial	
Week 4 : 18 March - 22 March	Lecture	International Cyber Law and Governance
	Tutorial	
Week 5 : 25 March - 29 March	Lecture	Information and Political Warfare
	Tutorial	
Week 6 : 1 April - 5 April	Lecture	The Attribution Problem
	Tutorial	
Week 7 : 22 April - 26 April	Lecture	The Operational Context
Week 8 : 29 April - 3 May	Lecture	Cyber security threats, vulnerabilities, and risks
	Laboratory	Windows 10 and Cyber Security– Basic Concepts
Week 9 : 6 May - 10 May	Lecture	Vulnerabilities, Threats and Countermeasures
	Laboratory	Vulnerable Systems, Attacks and How They Happen
Week 10 : 13 May - 17 May	Lecture	Networking and Secure Communications
	Laboratory	What has changed and is Windows 10 still vulnerable
Week 11 : 20 May - 24 May	Lecture	Social Engineering
Week 12 : 27 May - 31 May	Lecture	Critical Infrastructures and their protection (Recorded lecture due to compensation day)
Week 13 : 3 June - 7 June	Lecture	Part 1: Guest Lecture. Part 2: Revision and preparation for the final exam

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.unsw.edu.au/planning-assurance/conduct-integrity/conduct-unsw/student-conduct-integrity/student-code-conduct

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Convenor	Faycal Bou hafs		Room 213, Building 15,	02 5114 5124	Consultation at any time in working hours. Please phone or email to make an appointment.	No	Yes
	Sally Burt		Room 112, Building 28	02 5114 5328	Consultation at any time in working hours. Please phone or email to make an appointment.	No	No

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)