UNSW Course Outline

ZEIT8025 Reverse Engineering - 2024

Published on the 09 Feb 2024

General Course Information

Course Code : ZEIT8025
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

This course provides an introduction to reverse engineering. Topics covered include an introduction to the intel machine code and assembler language, OllyDbg and Virtualisation, the MalDB malware repository, the Malware Analysis Lexicon and the family of ICS/SCADA malware.

The basics of static and dynamic reverse engineering will be taught. Students will do exercises to gain familiarity with the tools and techniques necessary to reverse engineer software.

Course Aims

This course aims to:

1) Provide technical, operational and management staff at all levels with an advanced knowledge of malware reverse engineering.

2) Provide a better understanding of what cyber operations entail and how various actors conduct cyber operations in today's global cyberspace.

3) Provide practical experience in cyber operations using the UNSW Canberra Cyber Range

Course Learning Outcomes

Course Learning Outcomes
CLO1 : Understand the range of tools, techniques and technologies associated with reverse engineering.
CLO2 : Understand body of knowledge
CLO3 : Work independently and collaboartively
CLO4 : Produce scholarly output

Course Learning Outcomes	Assessment Item
CLO1 : Understand the range of tools, techniques and technologies associated with reverse engineering.	• One Quiz • Research Project - Academic Writing
CLO2 : Understand body of knowledge	• Minor Practical Assessment - Free Text Questions • One Quiz • Research Project - Academic Writing
CLO3 : Work independently and collaboartively	• Major Practical Assessment - Technical Report • Minor Practical Assessment - Free Text Questions • Research Project - Academic Writing
CLO4 : Produce scholarly output	• Major Practical Assessment - Technical Report • Research Project - Academic Writing

Learning and Teaching Technologies

Moodle - Learning Management System

Learning and Teaching in this course

This course relies on a variety of teaching strategies.

The concepts presented in this course require students' demonstration of skills including structured thinking and reverse engineering practice. Therefore, the teaching strategies employed in this course aim at providing an engaging and rewarding educational environment to facilitate the students' learning experiences through the development of expertise in reverse engineering.

The lecture notes are divided into modules to facilitate structured and scheduled studying activities.

During the semester, students will get a chance to work individually and in groups ona number of inclass exercises that will give them an opportunity to think about and attempt parts of the course assignments. The course convenor willbe available during these exercises to provide immediate feedback on their thinking and applied methods. This will provide students with a head- start for attempting their final assignment - Research Project.

The in-class exercises will also provide students with the opportunity to reflect on and refresh important concepts covered during the semester's workshops and prepare for the Quizzes.Quizzes are designed to provide a mechanism to test students' ability to remember important concepts learnt during the semester.

There is an expectation that students will all use MOODLE. MOODLE will provide mechanisms to facilitate online discussions between students. Students are encouraged to log on to MOODLE on a regular basis for updates relating to the course. It is expected that students will study as much of the recommended reading material as they can, as well as expand their reading through the linked references and their own research, reflect upon the studied material and think outside the box to comprehend the concepts and techniques taught in this course.

Additional Course Information

Course is going through an update and parts of the course outline may not be up to date. There will be no quizzes at the end of each week. Please refer to the assessment section for the latest

information on how the course teaching strategy will be. Please refer to the course Moodle for the latest updates.

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
One Quiz Assessment Format: Individual	10%	Start Date: Not Applicable Due Date: 15/03/2024 11:55 PM
Minor Practical Assessment - Free Text Questions Assessment Format: Individual	20%	Start Date: Not Applicable Due Date: Week 7: 22 April - 26 April
Major Practical Assessment - Technical Report Assessment Format: Individual	30%	Due Date: Week 10: 13 May - 17 May
Research Project - Academic Writing Assessment Format: Individual	40%	Due Date: 14/06/2024 08:00 PM

Assessment Details

One Quiz

Assessment Overview

Students will be given one hour to complete a theoretical task. The examination will be based on the covered lectures and labs content. Marking criteria: 1) completeness, 2) structure and coherence, and 3) depth and accuracy.

Course Learning Outcomes

- CLO1 : Understand the range of tools, techniques and technologies associated with reverse engineering.
- CLO2 : Understand body of knowledge

Detailed Assessment Description

Quiz

Assessment Length

45 Minutes

Submission notes

Multiple Choices

Assignment submission Turnitin type

This is not a Turnitin assignment

Minor Practical Assessment - Free Text Questions

Assessment Overview

Students are to analyse a given unknown binary using techniques learned during the course. Submission format is answer to some questions based on students' analysis. Marking criteria: 1) completeness, 2) structure and coherence, and 3) depth and accuracy.

Course Learning Outcomes

- CLO2 : Understand body of knowledge
- CLO3 : Work independently and collaboartively

Major Practical Assessment - Technical Report

Assessment Overview

Students are to analyse a given malware. Submission format is a technical report. Marking criteria: A detailed rubric is available in the Moodle.

Course Learning Outcomes

- CLO3 : Work independently and collaboartively
- CLO4 : Produce scholarly output

Research Project - Academic Writing

Assessment Overview

Students are to examine and discuss a recent paper in reverse engineering. Marking criteria: A detailed rubric is available in the Moodle.

Course Learning Outcomes

- CLO1 : Understand the range of tools, techniques and technologies associated with reverse engineering.
- CLO2 : Understand body of knowledge
- CLO3 : Work independently and collaboartively
- CLO4 : Produce scholarly output

General Assessment Information

Grading Basis

Standard

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 1 : 26 February - 1 March	Lecture	Lecture Chapter 1 - introduction • Malicious Actions • Malware Delivery and Exploitation • Malware C2
Week 2 : 4 March - 8 March	Lecture	Lecture Chapter 1 - introduction • Persistence and Evading Detection • Side Channel Attacks and Jumping Airgaps • Readings
Week 3 : 11 March - 15 March	Lecture	Lecture Chapter 2 - Object File Formats • Object File Formats • Compilation, Linking and Loading
Week 4 : 18 March - 22 March	Lecture	Lecture Chapter 2 - Object File Formats • Code to Assembly demo lecture • Object File Format: PE
Week 5 : 25 March - 29 March	Lecture	Lecture Chapter 2 - Object File Formats • Object File Format: PE Demo • Object File Format: ELF • Object File Format: ELF Demo • Object File Format: Java class
Week 6 : 1 April - 5 April	Lecture	Lecture Chapter 3 - Malware Analysis • Program Representation • Dynamic Analysis
Week 7 : 22 April - 26 April	Lecture	Lecture Chapter 3 - Malware Analysis • Program Analysis
Week 8 : 29 April - 3 May	Lecture	Lecture Chapter 3 - Malware Analysis • Binary Program Analysis
Week 9 : 6 May - 10 May	Lecture	Lecture Chapter 4 - Malware Classification • Program Similarity
Week 10 : 13 May - 17 May	Lecture	Lecture Chapter 4 - Malware Classification • Program Classification Using Machine Learning
Week 11 : 20 May - 24 May	Lecture	Lecture Chapter 4 - Malware Classification • Malware Obfuscation
Week 12 : 27 May - 31 May	Lecture	Lecture Chapter 4 - Malware Classification • Evasion, Code Packing Transformations and Unpacking

Attendance Requirements

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

Course Resources

Prescribed Resources

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

- Recommended papers and chapters fromtextbooks, Internet-based documents and other sources. In general, this will be made available through the Moodle course page.
- Lectures and presentation notes in the form of PDF slides covering the material presented during IDM week. These will also be made available through the Moodle course page.

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
	Dr. Pedram Hayati					No	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)