School of
Engineering and Computer Science
Te Kura Mātai Pūkaha, Pūrorohiko

Prescription

This course addresses the problem of using reverse-engineering techniques and related techniques such as fuzzing to both analyse malicious code and identify vulnerabilities in software. Topics will include methodology and techniques as well as the anatomy, behaviour and Propagation of malware. Practical work will involve malware analysis in a controlled environment as well as the analysis of real-world vulnerabilities and creation of exploits.

Course learning objectives

Students who pass this course should be able to:

1. Analyse the anatomy, behaviour and propagation methods of malware using reverse-engineering tools.
2. Detect and bypass attempts by malware to evade analysis.
3. Create a proof-of-concept exploit by identifying vulnerabilities in real-world software using fuzzing and related techniques.

Course content

2022: The course is primarily offered in-person, and there are components such as tests, labs, tutorials, and marking sessions which require in-person attendance. There will be remote alternatives for all the components of the course, but these are only available to students studying from outside the Wellington region. The remote option for tests will use a Zoom-based system for online supervision of the tests.

Students taking this course remotely must have access to a computer with camera and microphone and a reliable high speed internet connection that will support real-time video plus audio connections and screen sharing. Students must be able to use Zoom; other communication applications may also be used. A mobile phone connection only is not considered sufficient. The computer must be adequate to support the programming required by the course; we recommend a machine capable of running virtual machines. A mobile device such as a tablet or mobile phone will not be sufficient.

Withdrawal from Course

Withdrawal dates and process:
https://www.wgtn.ac.nz/students/study/course-additions-withdrawals

Lecturers

AProf Ian Welch (Coordinator)

ian.welch@vuw.ac.nz 04 463 5664

Harith Al-Sahaf

harith.al-sahaf@vuw.ac.nz 04 463 5656

CO 129 Cotton Building (All Blocks), Gate 7, Kelburn Parade, Kelburn

Teaching Format

This course will be offered in-person and online. For students in Wellington, there will be a combination of in-person components and web/internet based resources. It will also be possible to take the course entirely online for those who cannot attend on campus, with all the components provided in-person also made available online.

Weekly lectures and lab sessions during the whole course. Students will cover the fundamentals of malware analysis and reverse engineering techniques for malware in this context. The final assessment will involve applying a range of these techniques to a problem such as developing a proof-of-concept malware exploit.

Student feedback

You can view Student course feedback collected for the University courses from the last completed trimester for which feedback was collected

Dates (trimester, teaching & break dates)

- Teaching: 28 February 2022 - 03 June 2022
- Break: 11 April 2022 - 24 April 2022
- Study period: 06 June 2022 - 09 June 2022
- Exam period: 10 June 2022 - 25 June 2022

Class Times and Room Numbers

28 February 2022 - 10 April 2022

- **Tuesday** 11:00 - 11:50 – 319, Old Kirk, Kelburn
- **Friday** 11:00 - 11:50 – 319, Old Kirk, Kelburn

25 April 2022 - 05 June 2022

- **Tuesday** 11:00 - 11:50 – 319, Old Kirk, Kelburn
- **Friday** 11:00 - 11:50 – 319, Old Kirk, Kelburn

Other Classes

We will have online helpdesks from 3.10-4 pm in the weeks prior to the assessment due dates and will share the Zoom link with you during the course.

Set Texts and Recommended Readings

Required

- *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software* (1st edition) by

Michael Sikorski and Andrew Honig - available at no charge via the University O'Reilly online subscription.

Mandatory Course Requirements

In addition to achieving an overall pass mark of at least 50%, students must:

- Achieve at least a "**D**" in the final assignment.

If you believe that exceptional circumstances may prevent you from meeting the mandatory course requirements, contact the Course Coordinator for advice as soon as possible.

Assessment

This is the 2022 assessment scheme.

Assessment Item	Due Date or Test Date	CLO(s)	Percentage
Assignment one (3 weeks)	10th April 2022	CLO: 1	30%
Assignment two (3 weeks)	15th May 2022	CLO: 1,2	30%
Assignment three (4 weeks)	12th June 2022	CLO: 1,2,3	40%

Penalties

Each student will have 3 "late days" - 72 hours of automatic extension which will be applied to any assignment or assignments during the course, as needed. Please note that these 72 hours are for the whole course, not for each assignment.

The penalty for late work beyond your allocation of "late days" will be a 10% shrinking cap per day after the due date, unless there has been prior negotiation. Shrinking cap reduces the maximum mark per day so after 3 days the maximum mark is 70%(B) but C+ work will receive a C+ grade.

Extensions

Individual extensions will only be granted in exceptional personal circumstances, and should be negotiated with the course coordinator before the deadline whenever possible. Documentation (eg, medical certificate) may be required.

Submission & Return

All work should be submitted through the ECS submission system, accessible through the course web pages. Marks and comments will be returned through the ECS marking system, also available through the course web pages.

Workload

The student workload for this course is 150 hours.

Teaching Plan

See https://ecs.wgtn.ac.nz/Courses/CYBR473_2022T1/LectureSchedule

Communication of Additional Information

All online material for this course can be accessed at https://ecs.wgtn.ac.nz/Courses/CYBR473_2022T1/

Links to General Course Information

- Academic Integrity and Plagiarism: https://www.wgtn.ac.nz/students/study/exams/integrity-plagiarism
- Academic Progress: https://www.wgtn.ac.nz/students/study/progress/academic-progess (including restrictions and non-engagement)
- Dates and deadlines: https://www.wgtn.ac.nz/students/study/dates
- Grades: https://www.wgtn.ac.nz/students/study/progress/grades
- Special passes: Refer to the Assessment Handbook, at https://www.wgtn.ac.nz/documents/policy/staff-policy/assessment-handbook.pdf
- Statutes and policies, e.g. Student Conduct Statute: https://www.wgtn.ac.nz/about/governance/strategy
- Student support: https://www.wgtn.ac.nz/students/support
- Students with disabilities: https://www.wgtn.ac.nz/st_services/disability/
- Student Charter: https://www.wgtn.ac.nz/learning-teaching/learning-partnerships/student-charter
- Terms and Conditions: https://www.wgtn.ac.nz/study/apply-enrol/terms-conditions/student-contract
- Turnitin: http://www.cad.vuw.ac.nz/wiki/index.php/Turnitin
- University structure: https://www.wgtn.ac.nz/about/governance/structure
- VUWSA: http://www.vuwsa.org.nz

Offering CRN: 32241

Points: 15
Prerequisites: CYBR 271, 371, 30 further 300-level pts from (CYBR, NWEN, SWEN 324, 326)
Duration: 28 February 2022 - 26 June 2022
Starts: Trimester 1
Campus: Kelburn