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

The course is primarily offered in-person, but there will also be a remote option and there will be online alternatives for all the components of the course for students who cannot attend in-person.

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: a reasonably powerful windows, macintosh, or unix laptop or desktop computer should be sufficient, but an Android or IOS tablet will not.

If the assessment of the course includes tests, the tests will generally be run in-person on the Kelburn campus. There will be a remote option for students who cannot attend in-person and who have a strong justification (for example, being enrolled from overseas).
The remote test option will use Zoom for online supervision of the tests and you must be able to use Zoom with a camera, microphone, and screen-sharing. Students who will need to use the remote test option must contact the course coordinator in the first two weeks to get permission and make arrangements.

==========

Withdrawal from Course

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

Lecturers

Harith Al-Sahaf (Coordinator)

harith.al-sahaf@vuw.ac.nz 04 4635656

129 Cotton, Kelburn

Ian Welch

ian.welch@vuw.ac.nz 04 4635664

131 Alan MacDiarmid Bldg Gate 7 Kelburn Pde, 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 whole course. Students will cover fundamentals of malware analysis and reverse engineering techniques in this context. The final assessment will involve applying a range of these techniques to a problem such as developing malware that can evade anti-virus detection.

Student feedback

This is the first time we have run the course so there is no feedback to report upon.

Dates (trimester, teaching & break dates)

- Teaching: 05 July 2021 - 08 October 2021
- Break: 16 August 2021 - 29 August 2021
- Study period: 11 October 2021 - 14 October 2021
- Exam period: 15 October 2021 - 06 November 2021

Class Times and Room Numbers

05 July 2021 - 15 August 2021

- **Monday** 11:00 - 11:50 – 710, Von Zedlitz, Kelburn
- **Thursday** 11:00 - 11:50 – 710, Von Zedlitz, Kelburn

30 August 2021 - 10 October 2021

- **Monday** 11:00 - 11:50 – 710, Von Zedlitz, Kelburn
- **Thursday** 11:00 - 11:50 – 710, Von Zedlitz, Kelburn

Other Classes

We will have tutorial sessions at 10:00 am in CO139 on 6th August, 10th September, and 1st October.

Set Texts and Recommended Readings

Required

There are no required texts for this offering.

Mandatory Course Requirements

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

- Complete at least 80% of the assigned labs.
- 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 2021 assessment scheme.

Assessment Item	Due Date or Test Date	CLO(s)	Percentage
Assignment one (3 weeks)	15th August 2021	CLO: 1	30%
Assignment two (3 weeks)	19th September 2021	CLO: 1,2	30%
Assignment three (4 weeks)	17th October 2021	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 10% shrinking cap per day after the due date, unless there has been prior negotiation. Shrinking cap reduces 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_2021T2/LectureSchedule

Communication of Additional Information

All online material for this course can be accessed at https://ecs.wgtn.ac.nz/Courses/CYBR473_2021T2/

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: 05 July 2021 - 07 November 2021
Starts: Trimester 2
Campus: Kelburn