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

Prescription

Cryptographic mechanisms are widely deployed for communication and data protection. This course addresses how cryptographic mechanisms can be effectively used within larger security systems and how cryptographic mechanisms can be vulnerable in deployed systems. Topics covered include cryptographic primitives, cryptographic protocols, cryptanalytic techniques on primitives and protocols in deployed systems and attacks based upon common errors in use of libraries. Practical work will include best practice use of cryptographic libraries and attacks.

Course learning objectives

Students who pass this course will be able to:

1. Describe the security properties and different application areas of common cryptographic primitives and protocols.
2. Analyse, evaluate and correctly use the most appropriate cryptographic libraries to implement specified data protection requirements or security protocols.
3. Use cryptanalytic techniques and tools to analyse and identify security vulnerabilities in the implementation of data protection and security protocols.

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: almost any modern windows, macintosh, or unix laptop or desktop computer will 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

Jyoti Sahni

jyoti.sahni@vuw.ac.nz

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.

There are two lectures per week that will be recorded and starting from week four there will be weekly helpdesks will be both in person and provided over Zoom.

Student feedback

Student feedback on University courses may be found at:
www.cad.vuw.ac.nz/feedback/feedback_display.php

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

- **Thursday** 14:10 - 15:00 – LT301, New Kirk, Kelburn
- **Friday** 14:10 - 15:00 – LT122, Cotton, Kelburn

30 August 2021 - 10 October 2021

- **Thursday** 14:10 - 15:00 – LT301, New Kirk, Kelburn
- **Friday** 14:10 - 15:00 – LT122, Cotton, Kelburn

Set Texts and Recommended Readings

Required

The textbook for the course is:

- *Cryptography Engineering: Design Principles and Practical Applications* 1st Edition by Niels

Ferguson (Author), Bruce Schneier and Takayoshi Kohno

Mandatory Course Requirements

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

- Achieve at least a **D** in the test, because the test assesses understanding of concepts and what was learnt in assignments independently.

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

The assignments will apply theory learnt in the lectures while the test will be related to the lecture material and learning during the assignments. The test will be related to the lecture material and learning during the assignments.

Assessment Item	Due Date or Test Date	CLO(s)	Percentage
Implementation assignment (4 weeks).	15 Aug 2021	CLO: 1	35%
Analysis assignment (4 weeks).	3 Oct 2021	CLO: 2	35%
Test (2 hours).	Assessment week	CLO: 1,2,3	30%

Penalties

Late assignment submissions will receive a penalty of 10% for each day late (pro-rata).

Extensions

Each student will have three "late days" which you may choose to use for any assignment or assignments during the course. There will be no penalty applied for these late days. You do not need to apply for these, instead any late days you have left will be automatically applied to assignments that you submit late.

Submission & Return

All work is 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 total workload for CYBR 372 is 150 hours. In order to maintain satisfactory progress in CYBR 372, you should plan to spend an average of 10 hours per week on this course. An approximate breakdown is: lectures 2 hours, assignments 5 hours and assigned readings/review of notes 2 hours.

Teaching Plan

See: https://ecs.wgtn.ac.nz/Courses/CYBR372_2021T2/LectureSchedule

Communication of Additional Information

All online material for this course can be accessed at https://ecs.wgtn.ac.nz/Courses/CYBR372_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: 32078

Points: 15
Prerequisites: CYBR 171; CYBR 271 or COMP 261; NWEN 243
Duration: 05 July 2021 - 07 November 2021
Starts: Trimester 2
Campus: Kelburn