Course Outline

Contents

- Course Details
- Course Summary
- Assumed Knowledge
- Student Learning Outcomes
- Teaching Strategies
- Teaching Rationale
- Student Conduct
- Assessment
- Course Schedule
- Resources for Students
- Course Evaluation and Development

Course Details

Course Code	COMP4337
Course Title	COMP4337/9337 Securing Wireless and Wireless Networks
Convenor	Sanjay Jha (/users/z9902995)
Admin	Sanjay Jha (/users/z9902995)
Classes	**Lectures** : Wed 14-16 # (w1-5,7-10, Online) Timetable for all classes (/COMP4337/21T1/timetable)
Consultations	
Units of Credit	6
Course Website	http://cse.unsw.edu.au/~cs4337/21T1/ (http://cse.unsw.edu.au/~cs4337/21T1/)
Handbook Entry	http://www.handbook.unsw.edu.au/undergraduate/courses/current/COMP4337.html (http://www.handbook.unsw.edu.au/undergraduate/courses/current/COMP4337.html)

Course Summary

To provide an in-depth introduction to a wide range of topics in the field of Wireless Network Security. To get a hands-on understanding of the security issues in wireless networks.

Assumed Knowledge

Before commencing this course, students should:

- have completed COMP3331/9331
- have programming skills acquired in other subjects.

Student Learning Outcomes

After completing this course:

Students will have a sound knowledge of the state-of-the-art advances in network security, with an emphasis on the next generation Internet architectures and protocols. They will be able to demonstrate their knowledge both by describing aspects of the topics, and by solving problems related to the topics.

Students will also be equipped with the necessary skills to conduct security analysis of fixed and wireless networks.

A wide range of assessment components ranging from lab exercises, lab reports, oral presentation, research project will be used to measure these outcomes. This is explained in greater details in the description of the individual assessment tasks.

By completing the laboratory exercises and reports, the students will develop the following UNSW graduate attributes:(i) the ability to engage in independent and reflective learning because they will need to use the concepts learned in the lectures to design their program specifications individually and (ii) information literacy skills to appropriately locate, evaluate and use relevant information because they will need to use the programming skills and basic networking concepts previously acquired in earlier subjects.

This course contributes to the development of the following graduate capabilities:

Graduate Capability	**Acquired in**
Scholars capable of independent and collaborative enquiry, rigorous in their analysis, critique and reflection, and able to innovate by applying their knowledge and skills to the solution of novel as well as routine real world problems	the assignment has been specifically designed so that students can gain the required analytical skills for solving real world problems
Entrepreneurial leaders capable of initiating and embracing innovation and change, as well as engaging and enabling others to contribute to change	the students will have to work in a group to accomplish their goals, guest lectures from industry
Professionals capable of ethical, self- directed practice and independent lifelong learning	Labs, assignment, in-class interactions
Global citizens who are culturally adept and capable of respecting diversity and acting in a socially just and responsible way	interaction with your fellow students

Teaching Strategies

The main objective of this course is to encourage students to be creative and being able to think outside the box. Students should be able to relate new ideas to previous knowledge or real-world experience. The student experience will consist of recorded lectures for review, an online weekly interactive session for the first 7-8 weeks. The weekly online interactive session will consist of a short weekly quiz as a refresher on last week's lecture module, a Q&A session and review of difficult concepts as requested by students, sharing of interesting cybersecurity related news such as vulnerability, compromise in real world. COMP4337/9337 uses hands on laboratory sessions aimed at supporting problem-based learning to enhance student experience. The student experience will be supported by on-line access consultation by lab tutors and access to materials. Finally, students will be required to complete an assignment by writing programs, analysing security vulnerabilities propose solution, write and report and demonstrate their system. This term, the assignment will be based on developing a secure Covid Application.

Teaching Rationale

This course is an elective and focussed on acquiring basic theoretical network security skills as well as hands-on skills that will prepare students for the cybersecurity industry as well as R&D oriented jobs.

Student Conduct

The **Student Code of Conduct** (Information (https://student.unsw.edu.au/conduct) , Policy (https://www.gs.unsw.edu.au/policy/documents/studentcodepolicy.pdf)) sets out what the University expects from students as members of the UNSW community. As well as the learning, teaching and research environment, the University aims to provide an environment that enables students to achieve their full potential and to provide an experience consistent with the University's values and guiding principles. A condition of enrolment is that students *inform themselves* of the University's rules and policies affecting them, and conduct themselves accordingly.

In particular, students have the responsibility to observe standards of equity and respect in dealing with every member of the University community. This applies to all activities on UNSW premises and all external activities related to study and research. This includes behaviour in person as well as behaviour on social media, for example Facebook groups set up for the purpose of discussing UNSW courses or course work. Behaviour that is considered in breach of the Student Code Policy as discriminatory, sexually inappropriate, bullying, harassing, invading another's privacy or causing any person to fear for their personal safety is serious misconduct and can lead to severe penalties, including suspension or exclusion from UNSW.

If you have any concerns, you may raise them with your lecturer, or approach the School Ethics Officer (mailto:ethics-officer@cse.unsw.edu.au) , Grievance Officer (mailto:grievance-officer@cse.unsw.edu.au) , or one of the student representatives.

Plagiarism is defined as (https://student.unsw.edu.au/plagiarism) using the words or ideas of others and presenting them as your own. UNSW and CSE treat plagiarism as academic misconduct, which means that it carries penalties as severe as being excluded from further study at UNSW. There are several on-line sources to help you understand what plagiarism is and how it is dealt with at UNSW:

- Plagiarism and Academic Integrity (https://student.unsw.edu.au/plagiarism)
- UNSW Plagiarism Procedure (https://www.gs.unsw.edu.au/policy/documents/plagiarismprocedure.pdf)

Make sure that you read and understand these. Ignorance is not accepted as an excuse for plagiarism. In particular, you are also responsible that your assignment files are not accessible by anyone but you by setting the correct permissions in your CSE directory and code repository, if using. Note also that plagiarism includes paying or asking another person to do a piece of work for you and then submitting it as your own work.

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. Plagiarism undermines academic integrity and is not tolerated at UNSW. Plagiarism at UNSW is defined as using the words or ideas of others and passing them off as your own.

If you haven't done so yet, please take the time to read the full text of

- UNSW's policy regarding academic honesty and plagiarism (https://student.unsw.edu.au/plagiarism)

The pages below describe the policies and procedures in more detail:

- Student Code Policy (https://www.gs.unsw.edu.au/policy/documents/studentcodepolicy.pdf)
- Student Misconduct Procedure (https://www.gs.unsw.edu.au/policy/documents/studentmisconductprocedures.pdf)
- Plagiarism Policy Statement (https://www.gs.unsw.edu.au/policy/documents/plagiarismpolicy.pdf)
- Plagiarism Procedure (https://www.gs.unsw.edu.au/policy/documents/plagiarismprocedure.pdf)

You should also read the following page which describes your rights and responsibilities in the CSE context:

- Essential Advice for CSE Students (https://www.engineering.unsw.edu.au/computer-science-engineering/about-us/organisational-structure/student-services/policies/essential-advice-for-cse-students)

Communications:

This term, we are moving to Teams software. We strongly recommend Microsoft Teams channels for communication as appropriate. However, in some cases, if you students wish to use email, please use the following class E-Mail: eng.cse.comp4337@unsw.edu.au

(1) All students MUST read posts from the Microsoft Teams for any updates or notices regularly. Students must also check their UNSW (or redirected) e-mail regularly for announcements regarding this course. Please note that we are using Teams for course delivery and improved learning. Missing a notification is not a valid excuse at any point.

(2) Students must follow the proper communication channels. These are clearly specified on Moodle/Teams.

Note: ***Do not send direct emails to LIC, Administrator, etc. via their personal email addresses. Emails received at private accounts will not be read and automatically deleted without reply unless confidentiality is required.***

Special Considerations/ Supplementary Examination:

All students with approved letter from UNSW Disability Support must upload their letters through the designated link on Moodle. Students should not use email for such requests. The Course Admin will reply to the student letter issued from Disability Support and will apply any requirement specified in the letter throughout the semester.

For any unexpected incident that the student requires Special Consideration (e.g. illness affecting reaching a deadline, or missing a Quiz), the student must submit a Special Consideration request through the designated link on Moodle. In fact, as per the university policy, all Special Consideration requests have to be submitted through the central system. Hence, please refer to the designated link on Moodle and follow the instructions. Your LIC will decide as per documents you provide there. Email requests about special consideration sent to course admin and LIC will not be attended to.

The following cases may be considered:

(1) A student has submitted a fully documented request for Special Consideration within 3 days of the assignments or assessments. The medical or other evidence is clearly of a nature to affect the student's performance seriously (minor ailments such as cold, headache - unless chronic, or severe enough to require prescribed medication, will not be considered). Feeling 'unwell', for instance does not excuse a poor result. In simple terms, not all applications are automatically accepted.

(2) A student's performance during the semester, particularly in the lab and assignment reports has been of satisfactory standard. Students who perform poorly in such assessment components will not be granted a supplementary exam for missing quizzes.

(3) A supplementary assessment will be arranged at a suitable time by the school/lecturer-in-charge.

If you miss a quiz-1, we will not be able to organise a supplementary. We will offer scaling up your second quiz-2 .

Re-Assessment Policy: The University has a policy for review of results that allows students who believe there has been an error in the calculation of their final mark to appeal that mark. There currently may be a fee attached to applying for a re-mark which is refunded only if the mark changes substantially upwards. UNSW Student Central will advise of the current policy on applying this fee. There is also a 15 working day time limit in applying for a review of marks. See: https://student.unsw.edu.au/results.

Students are able to apply for an "administrative check" that all sections of their final exam have been marked, and all marks and assessment task marks have been correctly entered into the calculation of the final mark. The fee for this is nominal.

Students may also apply for a "re-assessment" or "re-mark" of a piece of work. The fee for this is substantial. The re-mark is done using the same marking scheme as was used originally. Normally this will be done by a person other than the original marker. If the re-marker feels that an error in marking has been made then they will consult with the original marker where relevant as to the correct interpretation of the mark scheme.

A re-mark may result in the allocated mark increasing, staying the same or decreasing.

Students should note that it is rare in a large class for there to be a change in the mark following a re-mark. Before applying for a re-mark the student should have consulted with the Course Convenor on their performance in the course.

Assessment

Item	Topics	Due	Marks	Contributes to
Quizzes	All topics	TBA	30%	1,2,...
Assignment	Security Analysis	TBA	30%	1,...
Labs	All topics	5-6 Labs, Weeks TBA	30%	1,2,...
Class Participation		Weekly	10%	1,2,...

Note:

A double pass is applicable to this course where students must achieve 40% in the combined marks of two quizes to pass this subject. Students achieving less than 40% in the combined quiz1 and quiz2 marks (i.e. 12/30), will have their final total marks capped to maximum of 50 (Pass). There is no final examination in this subject.

Class Participation Marks :

This will be allocated for participation in the weekly online interactive sessions, posing and answering questions related to lecture material, attempting short weekly quiz, participation in Q&A over teams, asking/answering questions on Teams channels, contributing to news items and other course related resources on “News” channel.

Course Schedule (*Tentative, please follow Teams channels for changes*)

Week	Lectures	Tutes	Labs	Assignments	Quizzes	Notes
1	Course Overview, Security in IP protocol stack Network Security, Crypto intro	No	No	-	-	-
2	Wireless LAN, Stream Ciphers, symmetric key ciphers	No	Lab1-crypto	-	-	-

3	Authentication, Key distribution/Kerberso, PGP, SSL, TLS, PKI	No	-	-	-	-
4	Network Layer Security, IPSec	No	Lab2- Wireless Net	-	-	-
5	Authentication and Authorisation in WLAN, 801.X EAP	No	Lab3 -MiTM, Evil Twin	Ass. release	Quiz 1	-
6	Mid-term break	-	-	-	-	-
7	Intrusion Detection/Prevention System, Machine learning applied to Security	No	Lab4- Sec Analysis Wireshark	-		-
8	Introduction to BluetoothSecurity Broadcast Authentication, MerkleTree , IoT Security	No	Lab5- Snort IDS	-	-	-
9	Blockchain Security, Privacy Techniques	No	Lab6- BLE	-	-	-
10	Guest Lecture, Project work/demo/submission	No	Lab7- (Tentative)	-	Quiz 2	-
11	Revision	No	-	-	-	-
	* **Due dates tentative please check notice/specs**					
	*** Lecture order may change, new topics via guest lecture**					

Resources for Students

Texts and recommended readings:

<o:p></o:p>This course does not have a prescribed textbook. Most of the content presented will multiple books, on-line materials, conference proceedings, journal articles, etc. A list of references related to each week's lecture content will be made available on the course webpage.

Students are expected to read articles/papers as directed. Lecture notes will have reference to appropriate sections (and other material)

The following is a list of reference textbooks, which may be useful. Students are not required to purchase these.

- William Stallings, Cryptography and Network Security, Sixth Edition
- Security in Fixed and Wireless Networks: Guenter Schaefer, Michael Rossberg, Wiley, 2nd Edition, 2016
- CWSP – Certified Wireless Security Professional Official Study Guide
- R. Nichols and P. C. Lekkas, Wireless Security: Models, Threats and Solutions., McGraw-Hill Telecom, 2006
- M. Spincer, R. Perlman and C. Kaufman, Nework Security” Private Communicaton in a Public Worked, Pearson Ed, 2002

- L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks

Other resources

- Students will find the following Network Security Knowledge Area (and other KAs from this site) useful for this subject and other security topic: **https://www.cybok.org/** <o:p></o:p>

Course Evaluation and Development

Student feedback on this course, and on the lecturing in this course, will be gathered via myExperience portal. Student feedback is taken seriously, and continual improvements are made to the course based in part on this feedback. The course questionnaire results go to the Head of the School of Computer Science and Engineering, who reads the results and follows up in cases where action is clearly needed

In addition, feedback may also be gathered during the term to gauge the student experience and make any quick changes if required to improve student learning.

The course had highly positive feedback in T1 2020 despite the impact of COVID. There have been requests for improved in-class interactions, we are implementing a weekly interactive session to accommodate this.

Resource created 4 months ago (Monday 15 February 2021, 10:32:26 AM), last modified 4 months ago (Monday 15 February 2021, 01:09:28 PM).

Comments

(/COMP4337/21T1/forums/search?forum_choice=resource/58369)

(/COMP4337/21T1/forums/resource/58369)

There are no comments yet.