COMP4337/9337 Securing Wireless Networks

SUBJECT OUTLINE
Term 1 2019
Date of Modification:11th Feb 2019
Date of Creation: 7th February 2019

Staff Contact Details

Lecturer-in-Charge (LIC):
Prof Sanjay Jha
Office: K-17, Room501A, Level 5
Phone: 9385 6471
E-mail: eng.cse.comp4337@unsw.edu.au
Consultation Time: By Appointment

Guest Lecturer: Arash Shaghaghi, Wanli Xue, Weitao Xu

Course Admin and Head Tutor: Ms Uzma Maroof
Lab Tutor: Rizka Purwanto

Teaching Platform: Moodle. Access to Moodle is granted by UNSW central systems and course staff have no access to change this. All students are expected to read and follow material posted on the course Moodle page.
There will be no submission or mark provision through CSE GIVE system and all communications occur through Moodle.

Course Information
Units of Credit: 6
Parallel Teaching: This is a combined undergraduate and postgraduate course.
Pre-requisites:
COMP3331/9331

Aims:
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.

Learning Outcomes: The following are the student learning outcomes:

- Students successfully completing this course will have a sound knowledge of the state-of-the-art advances in wireless 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 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.
- By completing the project, the students will develop the following UNSW graduate attributes: (i) the capacity for analytical and critical thinking for creative problem-solving because the project have been specifically designed so that students can gain the required analytical skills for solving real world problems and (ii) the skills required for collaborative work because the students will have to work in a group to accomplish their goals. (iii) By presenting/demonstrating their project, the students will develop the skills for effective communication.

Teaching Strategy: 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 lectures (3-4 hrs per week) for the first 7-8 weeks. A set of review/quiz questions is provided to help reinforce the main ideas introduced during the lecture (There are no formal tutorials in this course). At least some part of assessment should be based on real world experiences. COMP9337 uses of hands on laboratory sessions aimed at supporting problem based learning to enhance student-learning experience. The student experience will be supported by on-line access to materials. Finally, students will be required to complete a project by either writing programs, analyzing security vulnerabilities propose solution or a research report (Details TBA) .

Course Schedule

Lectures: 3 - 4 hours per week for 7- 8 weeks, Please check your student calendar. The lecture slot for the last few weeks may be used for final project related activities.

Laboratory sessions: 2-hour for 4 –5 weeks. One of the labs would be on Penetration Testing Wireless Networks, where all students are required to break a WEP and WPA/WPA2 network using tools such as Aircrack. Another lab is about running a MITM against TLS connections, where students use a range of different tools to setup a real attack scenario (Rogue Access Point setup and many more interesting PenTest skills). There may be up to 1 more lab this session. Please check the course page for updated information.

All labs will be in groups. In other words, students work in groups during lab times and submit their answers, each group submission is marked and all members receive the same mark. Hence, students must form groups and register them through Moodle using designated link. Students who do not report a group will be randomly matched together. Please refer to Moodle for detailed instructions about Lab submissions. Only one submission from group members is required. Please add student-id/name of all group members and follow any other requirement specified on Moodle when submitting your files.

Tutorials: There are no tutorials for this course.

Consultations: In addition to lectures and labs, there will be an optional consultation slot. Check the web page for timings. Students having difficulty with these timings may negotiate for a different slot with the LIC. There will be separate consultation for project and a tutor will be allocated to help with this task.

Lecture Topics:
With exponential growth of the Internet, security of a network has become increasingly challenging. This subject will explore the security vulnerabilities in both fixed and wireless networks and cover the fundamental concepts and advanced issues with an emphasis on the Internet architecture and protocols.
The following key concepts will be covered: Wireless Communications and Security overview, Review of Cryptographic techniques, 802.11 Technologies and legacy 802.11 Security: lessons learnt, Encryption Ciphers and Methods in Wireless Networks, Wireless Security Risks, Wireless Security Auditing and Pen Test Introduction, IPSec and IP layer security, PKI/X.509, Transport Layer Security/DTLS, Intrusion Detection and Protection Systems, Network Firewalls, Secure Neighbor Discovery, Routing and Forwarding Security, Authentication and Key Management in Wireless Networks/Sensor Networks, Broadcast Security and Secure Code Dissemination, Network Privacy and Anonymity, Security and Privacy in Location Services, Smart Grid and IoT security.

Lecture Schedule: The following table lists the tentative weekly schedule. Students will be informed of any changes during the lecture and by announcements on the notices page.

Week	Topics
1 (20-21st Feb)	a. Course Overview, b. Wireless Communications and Security Overview c. 802.11 Technologies and legacy 802.11 Security: lessons learnt
2 (27-28th Feb)	a. Encryption Ciphers and Methods in Wireless Networks. b. Wireless Basics
3 (6-7th March)	c. PKI and Transport Layer Security, DTLS

4 (13th -14th March)	a. IPSec, Comparison with TLS b. Authentication and Authorisation in WLAN, 801.X EAP
5 (20th -21st March)	a. Introduction to Bluetooth Security b. Broadcast Authentication, Merkle Tree
6 (27th-28th March)	a. IoT Security /Demo/Guest Lecture
7 (3rd- 4th April)	a. Intrusion Detection/Prevention System/Guest Lecture
8 (10th- 11th April)	a. Insider Threats in Network Security/Guest Lecture
9 (17th- 18th April)	b. Project work/demo/submission
10 (24th- 25th April)	c. Project work/demo/submission

A detailed course schedule will be available via the course webpage on Moodle. Order of guest lectures may change.

Student Resources

Textbook: 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)

Students will find the following Network Security Knowledge Area (and other KAs

from this site) useful for this subject and other security topics:

https://www.cybok.org/

Reference Texts:

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

- 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

Software Availability:

TBA

Assessment
There will be 3 assessment components as described below:

1 - **Lab Assignments**. After completion of labs, students will be asked to perform some task in their own time and submit for marking. Please check lab page for details. Check the Labs link on the course webpage for the exam schedule. The lab assessment will be marked out of **20** marks. Each student must attend the lab **ONLY** in his/her allocated lab session.

2 – **Project** (**20** marks)

This project will be done in a group of two. You will have 3-4 weeks to finish this project. Groups may choose to do either an implementation (coding) project or a research report. Please check the details and specification to be announced on course web site. Project deadlines will be advertised mid-semester.
(**Note**: that we could readjust the marking components between lab assignments and project in consultation with class)

Subject policy on project: The projects are an integral part of the assessment. Make sure that you submit your work on time. Follow the submission directions in the project carefully. Late submissions will be penalised according to the rules specified in the assignment specifications.

3 – **Attendance and class participation including Quizzes:** This component will contribute to a maximum of **20** marks. *There will be multiple in-class Quizzes without prior notice.* There will be no supplementary for missed quiz. If a special consideration is approved, your final exam will be scaled.

4 **Final Examination**. The format and details will be announced. The exam will take place during the university exam period. This component will contribute to a maximum of **40** marks. *Students must score at least **20** marks in the final exam to pass this subject.*

Academic Honesty and Plagiarism

All submissions are routinely subject to scrutiny for similarities with other students' assignments. If you copy from another person, or get an unreasonable amount of help from a friend (so your assignment begins to look like theirs), or if you work very closely with someone, there is a good chance we will detect it. When we do, you will be penalised. At the very least, you will lose some or all marks for that assignment. In the past, students have been automatically failed for submitting stolen assignments. Further details of the School plagiarism policy can be found here. (You acknowledged receipt of these rules when you obtained your CSE computer account, and the link above is for your convenience so that you can review the rules now.)

We are aware that a lot of learning takes place in student conversations, and don't wish to discourage those. However, it is important, for both those helping others and those being helped, not to provide/accept any programming language code in writing, as this is apt to be used exactly as is, and lead to plagiarism penalties for both the supplier and the copier of the codes. Write something on a piece of paper, by all means, but tear it up/take it away when the discussion is over.

If you are new to studying in Australia, be aware that attitudes to plagiarism at UNSW may be different from those in your home country. Make sure you are clear about the rules here at UNSW. In brief, and for the purposes of COMP4337/9337, plagiarism includes copying or obtaining all, or a substantial part, of the material for your assignment, whether programming language code, or written or graphical report material, without written acknowledgement in your assignment from:

1. a location on the internet;
2. a book, article or other written document (whether published or unpublished) whether electronic or on paper or other medium;
3. another student, whether in your class or another class;
4. a non-student (e.g. from someone who writes assignments for money)

Note also that there is a big difference between being able to understand someone else's code, and writing that code yourself from scratch. A computer programmer has to be able to write code from scratch. The assignments provide opportunities for you to develop the skills necessary to write your own networking code. Use these opportunities!
Further details on the CSE student plagiarism policy can be found here.

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 examination. 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 research reports has been of satisfactory standard. Students who perform poorly in such assessment components will not be granted a supplementary exam.
(3) A supplementary assessment will be arranged at a suitable time by the school/lecturer-in-charge.

If you miss a quiz, we will not be able to organise a supplementary. We will offer scaling up your final exam grades subject to meeting the special consideration policy.

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.

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 will also be gathered mid-way through the session to gauge the student experience and make any quick changes if required to improve student learning.

The course had highly positive feedback in 2017. Students had concern about use of Acadly platform. We have decided to move to Moodle this year. Also, there have been requests for improved in-class interactions. This is a two-way process; we will brainstorm some ideas on this at the start of lecture. Lab and project specification and submission requirements will be improved to make them more effective.

Communications via E-Mail

(1) All students MUST read 'Notices' from the course web-site for any updates or notices regularly. Students must also check their school e-mail regularly for announcements regarding this course. Please note that we are using **Moodle** for course delivery and improved learning. Students must check Moodle regularly. 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.

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. All communications must occur through Moodle.**

Further Information

- Students enrolled in COMP4337/9337 are expected to attend all classes
- The use of School of Computer Science and Engineering computing laboratories is subject to rules described in the Yellow Form, which you acknowledge (electronic) receipt of when you receive your computing account. The Yellow Form also outlines what to do in case illness or misadventure that affects your assessment, and supplementary examinations procedures within the School of Computer Science and Engineering.
- Information on UNSW Occupational Health and Safety policies and expectations
- Equity and Diversity issues