TELE3119
Trusted Networks
Course Outline – Semester 2, 2018

Never Stand Still | Faculty of Engineering | School of Electrical Engineering and Telecommunications

Course Staff

Course Convener: Prof. Aruna Seneviratne, MSEB 541, a.seneviratne@unsw.edu.au
Tutor: Prof. Aruna Seneviratne, MSEB 541, a.seneviratne@unsw.edu.au
Laboratory Contact: TBC

Consultations: You are encouraged to ask questions on the course material, before or after the lecture class times in the first instance, rather than via email. Lecturer consultation times will be advised during lectures. You are welcome to email the laboratory demonstrator, who can answer your questions on this course and can also provide you with consultation times. All email enquiries should be made from your student email address with "TELE3119" in the subject line, otherwise they may not be answered.

Keeping Informed: Announcements may be made during classes, via email (to your student email address) and/or via online learning and teaching platforms – in this course, we will be using the course webpage http://subjects.ee.unsw.edu.au/tele3119/. Please note that you will be deemed to have received this information, so you should take careful note of all announcements.

Course Summary

Contact Hours

The course consists of 3 hours of lectures, a 1-hour tutorial session every even week (starting from week 2) and a 1-hour laboratory session every odd week (starting from week 3).

Lectures	**Day**	**Time**	**Location**
	Monday	1300 -1500	RedC M032
	Wednesday	1400 - 1500	Mat310
Lab	Tue	1000-1300	ElecEng426
Tutorial	Wednesday	1300 – 1400	ElecEng 426

Context and Aims

This course is for 6 Units of Credit and aimed at Undergraduate Engineers wishing to understand security issues in communication networks. This course is designed to provide an integrated focus for security related aspects of networking, as a core competency for telecommunications engineers. More specifically, the course is intrinsically linked to the concepts, protocols, and networking fundamentals developed in Tele3118 and TELE4642. The networking issues covered in Tele3118/Tele4642 are re-analyzed from the standpoint of trust, authentication, integrity and security. A thorough knowledge and understanding of the principles underlying trust and security in modern telecommunication networks is considered a paramount networking skill. As such, this course is core for all Telecommunication students.

Indicative Lecture Schedule

Period	Summary of Lecture Program
Week 1	Introduction, Cryptography and Security concepts
Week 2	Secret key cryptography
Week 3	Message integrity and Hash functions
Week 4	Public key cryptography (RSA, Diffie-Hellman, Digital Signature); **Quiz 1**
Week 5	IPSec, VPN, Wireless Security
Week 6	SSL/TLS, PKI
Week 7	Email Security, PGP, Anonymized routing
Week 8	Intrusion detection and Firewall; **Quiz 2**
Week 9	Security Threats for IoT Systems
Week 10	Public Holiday & Protecting IoT Systems
Week 11	Threat Analytics
Week 12	Advanced communication security & Guest Lecture
Week 13	Review; **Project presentations**

Indicative Laboratory Schedule

Period	Summary of Laboratory Program
Week 3-5	Lab 1: Traffic analysis using Wireshark
Week 6-9	Lab 2: Profiling security vulnerabilities of an IoT device
Week 9-13	Lab 3: Project

Assessment

Laboratory Practical Experiments	30%
Quizzes	30%
Final Exam (2 hours)	40%

Pass in the Final Exam is a *mandatory* requirement to pass the course

Course Details

Credits

This is a 6 UoC course and the expected workload is 10 hours per week throughout the 13-week semester. It includes lectures and laboratories. Supervised labs (1 hour per week) will commence in week 3. However, you will be expected to work on the assignments and projects outside of designated lab hours.

Relationship to Other Courses

This is a 4th year undergraduate elective course in the School of Electrical Engineering and Telecommunications. It may also be taken by postgraduate students.

Course Objectives & Learning Outcomes

At the end of the course students should:

a) Understand the theory, concepts and challenges of encryption protocols
b) Understand the theory, concepts and challenges of authentication protocols
c) Understand how applications actually operate over communication networks
d) Understand key objectives in designing and analyzing a secured network
e) Be able to design and simulate the behavior of security in communication networks
f) Design secure and trusted network applications, and design web-based applications running over Secure Sockets Layer
g) Design network authentication systems and possess the ability to analyze network traffic from a security standpoint.

Relation to other courses:

This course is related to another communication courses offered by Electrical Engineering in that it builds on concepts and principles introduced in Tele3118. More specifically, the course is intrinsically linked to the concepts, protocols, and networking fundamentals developed in Tele3118. The networking issues covered in Tele3118 are re-analyzed from the standpoint of trust, authentication, integrity and security.

Graduate Attributes:

This course will impact on the following graduate attributes

1. Development of skills involved in scholarly enquiry
2. Capacity for analytical and critical thinking and for creative problem-solving
3. The ability to engage in independent and reflective learning
4. Information literacy - the skills to appropriately locate, evaluate and use relevant information

Teaching Strategies

Delivery Mode

The teaching in this course aims at establishing a good fundamental understanding of the areas covered using:

- Lectures – to give the basic material, discuss the intuition behind the mathematics, and learn to incorporate rigour in the solution process.
- Tutorials – to learn problem-solving techniques, employ critical thinking, and reflect and discuss alternative techniques.

- Labs – laboratory assignments will provide hands-on experience of network security, and an opportunity for constructing and evaluating practical tools.
- Project – will use group-work as a means of exploring a research problem in greater depth, and provide you with the opportunity to demonstrate and communicate your approach and solution.
- Quizzes – will provide feedback on your progress in problem-solving.
- Final examination – final test of competency.

Learning in this course

You are expected to attend all lectures, labs, and quizzes in order to maximise learning. You must prepare well for your laboratory classes and your lab work will be assessed. In addition to the lecture notes, you should read relevant sections of the recommended text. Reading additional texts will further enhance your learning experience. Group learning is also encouraged. UNSW *assumes* that self-directed study of this kind is undertaken in addition to attending face-to-face classes throughout the course.

Laboratory program

The laboratory schedule is deliberately designed to provide practical, hands-on exposure to the concepts conveyed in lectures soon after they are covered in class. You are required to attend laboratory every odd week starting from Week3.

Laboratory Exemption

There is no laboratory exemption for this course. Regardless of whether equivalent labs have been completed in previous courses, all students enrolled in this course must take the labs. If, for medical reasons, (note that a valid medical certificate must be provided) you are unable to attend a lab, you will need to apply for a catch-up lab during another lab time, as agreed by the laboratory coordinator.

Assessment

The assessment scheme in this course reflects the intention to assess your learning progress through the semester. Ongoing assessment occurs through the lab checkpoints (see lab manual), lab exams and the mid-semester exam.

Laboratory Assessment

- Assignment 1 [10%]: This assignment will require you to capture and analyse encrypted/unencrypted traffic. Grading will be based on correctness, and functionality.
- Assignment 2 [10%]: This assignment will involve security analysis and launch of attack to an IoT device to be demonstrated in lab session by week 9. Grading will be based on correctness, functionality, and novelty of design.
- Project [15%]: This project will be done in groups of up to 3 students, and is designed to train you in conducting team research into a topic. Groups will choose from a given list of topics or propose their own in consultation with the course convenor. The chosen topic will be briefly presented to the class in week 9. The final presentations will be done in week 13.

Quizzes

This course will have two in-class written quizzes that will evaluate and provide feedback on your understanding of the material in this course. Quiz 1 will be held in week 4 (Thu), and quiz 2 in week 8 (Thu). Each quiz is worth 15% of the final grade, and each will typically test your problem-solving skills. Re-tests will not be granted in the event that a student misses the test, unless satisfactory written evidence is presented of adverse conditions that prevented the student from taking the test. In such a case, the course convenor may at his sole discretion conduct the re-test orally (instead of or in addition to a written component) individually with the student, within two weeks of the original test date

Final Exam

The exam in this course is a standard closed-book 2 hour written examination. University approved calculators are allowed. The examination tests analytical and critical thinking and general understanding of the course material in a controlled fashion. Questions may be drawn from any aspect of the course (including laboratory), unless specifically indicated otherwise by the lecturer. Marks will be assigned according to the correctness of the responses.

Pass in the Final Exam is a mandatory requirement to pass the course

Course Resources

Textbooks

The class will not follow one text book, but will consist of material taken from various sources, including text books, online material, and other literature.

However, the course will follow to a large extent a significant fraction of:

- William Stallings, Lawrie Brown, Computer Security: Principles and Practice, 3rd Edition, Pearson, 2015.

Another good text (particularly the substantial chapter on security) well worth looking at is:

- James F. Kurose and Keith W. Ross, "Computer Networking: A Top-Down Approach", Global Edition (7e), Pearson Higher Ed, 2016.

Kurose & Ross is a particularly good book for you to revise the material of Tele 3118, which is a prerequisite for this class. You are supposed to be very familiar with the standard networking

material contained in Chapters 1 through 5 of Kurose & Ross – we will not cover this standard material in class.

Additional reference material and papers will be detailed in class.

Other Matters

Academic Honesty and Plagiarism

Plagiarism is the unacknowledged use of other people's work, including the copying of assignment works and laboratory results from other students. Plagiarism is considered a form of academic misconduct, and the University has very strict rules that include some severe penalties. For UNSW policies, penalties and information to help you avoid plagiarism, see http://www.lc.unsw.edu.au/academic-integrity-plagiarism. To find out if you understand plagiarism correctly, try this short quiz: https://student.unsw.edu.au/plagiarism-quiz.

Student Responsibilities and Conduct

Students are expected to be familiar with and adhere to all UNSW policies (see https://my.unsw.edu.au/student/atoz/ABC.html), and particular attention is drawn to the following:

Workload

It is expected that you will spend at least **ten to twelve hours per week** studying a 6 UoC course, from Week 1 until the final assessment, including both face-to-face classes and *independent, self-directed study*. In periods where you need to need to complete assignments or prepare for examinations, the workload may be greater. Over-commitment has been a common source of failure for many students. You should take the required workload into account when planning how to balance study with employment and other activities.

Attendance

Regular and punctual attendance at all classes is expected. UNSW regulations state that if students attend less than 80% of scheduled classes they may be refused final assessment.

General Conduct and Behaviour

Consideration and respect for the needs of your fellow students and teaching staff is an expectation. Conduct which unduly disrupts or interferes with a class is not acceptable and students may be asked to leave the class.

Work Health and Safety

UNSW policy requires each person to work safely and responsibly, in order to avoid personal injury and to protect the safety of others.

Special Consideration and Supplementary Examinations

You must submit all assignments and attend all examinations scheduled for your course. You should seek assistance early if you suffer illness or misadventure which affects your course progress. All applications for special consideration must be **lodged online through myUNSW within 3 working days of the assessment**, not to course or school staff. For more detail, consult https://student.unsw.edu.au/special-consideration.

Continual Course Improvement

This course is under constant revision in order to improve the learning outcomes for all students. Based on feedback from past years we will endeavor to provide more support for programming aspects of the lab work. Please forward any feedback (positive or negative) on the course to the course convener or via the online student survey MyExperience. As a result of previous feedback obtained for this course and in our efforts to provide a rich and meaningful learning experience, we have continued to evaluate and modify our delivery and assessment methods.

Administrative Matters

On issues and procedures regarding such matters as special needs, equity and diversity, occupational health and safety, enrolment, rights, and general expectations of students, please refer to the School and UNSW policies:
https://www.engineering.unsw.edu.au/electrical-engineering/resources/undergraduate-resources/policies-and-procedures
https://my.unsw.edu.au/student/atoz/ABC.html