Tele3119 Trusted Networks
Course Outline 2008
Pre-requisite: TELE3118

Staff Contact: Dr Robert Malaney,
Email: r.malaney@unsw.edu.au

Course Overview:
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. The networking issues covered in Tele3118 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.

Syllabus:
The course will cover the following material; Authentication Protocols in Networks; Network Application Security (Email, VoIP), IP Security (IPsec), IP Address Spoofing, ARP Security; Securing Network Routing Protocols; Securing Network Transport Protocols; Security Specific Architectures/Protocols (TLS, SSL, Radius/Diameter, 802.11i), Network Firewalls; Network Management Security Issues (SNMPv3), Securing QoS in Networks, Principles of Public-Key and Symmetric Key Cryptography.
**Course Objectives:**
At the end of the course students should:

a) Understand the theory and concepts behind encryption protocols
b) Understand the theory and concepts behind authentication protocols
c) Understand the theory and concepts behind other network security protocols
d) Understand key objectives in designing and analyzing a secured network

**Learning Outcomes:**
At the successful completion of the course the student should be able to:

a) Design secure and trusted network applications
b) Design web based applications running over Secure Sockets Layer
c) Design network authentication systems
d) Possess the ability to analyze network traffic from a security standpoint.

**Teaching Methods**
Lectures + Tutorials + Labs

**Lectures:**
You are strongly encouraged to attend all class lectures. There will be no formal notes handed out for class that covers all the class material in detail, and therefore you are requested to take your own notes during class. There may be occasional power-points put on the class web site for download but these will not be sufficient for you to cover the class material. The lectures will consist of some power-point presentations, discussion of material in prescribed texts, discussion of case studies, and discussion of problems sheets. Some material presented in class will not be available for download from class web site. You are strongly encouraged to participate in class by interacting through questions and discussions of class material, and to prepare before class by reading ahead and preparing solutions to class problems. There may be the occasional guest lecturer who works or researches in the area of network security.

**Prescribed Texts:**
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

Another good text (particularly the substantial chapter on security) well worth looking at is:- *J. Kurose & K. Ross: Computer Networking: 3rd (or 4th) Edition. A Top-Down Approach Featuring the Internet, Publisher: Addison-Wesley, 2007.*
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.

**Laboratories.**
The laboratory work is a compulsory part of the course. You must attend all labs. Non-attendance at a laboratory will result in zero marks for that lab. Details of the lab contents will be discussed in class. However, in broad terms you will be utilizing packet sniffers (Wireshark) to analyze network security threats, creating your own TCP/UDP socket programs, and designing and constructing (using your socket programs) a realistic secure authentication service along the lines of the protocols discussed in class. These labs will be done on an individual basis. All lab work must be completed by due dates. There will be zero marks for late work.

**Assessment Weighting:**
- **Final Examination (60%):** The examination is of three-hour duration, covering all aspects of the course that have been presented in lectures, tutorials, and labs. This exam will assess both understanding and analytical skills. You must pass this exam to pass course.
- **Mid-Session Test (20%):** The mid-session test will last 45 minutes and will be held in week 6. It will cover material covered in the course in week 1 to 6, and will test your conceptual understanding of this material, as well as your ability to apply the concepts to solving problems. This is compulsory test. There are zero marks for non-attendance at the mid-term.
- **Laboratory Assessment (20%):** There are six lab tasks, which will be assessed in terms of written reports of lab work, and testing of software developed during labs.

**Consultations**
Please make an appointment for consultation at other times beyond standard class consultations through e-mail to r.malaney@unsw.edu.au (all email must be from a UNSW student account). Standard consultation time is immediately after the lecture on Monday at 11am.

**Other Course Resources.**
Please see class web site [https://subjects.ee.unsw.edu.au/tele3119](https://subjects.ee.unsw.edu.au/tele3119) for other material. It is expected and assumed that you will check this web site at least once per week for important class announcements.

**Plagiarism is strictly prohibited.**