Tele3119 Trusted Networks  
Course Outline Session 2, 2010  

Instructor: Dr. Ashay Dhamdhere  

Course Aim  
The main aim of this course is to develop a solid understanding of the key concepts and principles behind security and authentication protocols in communication networks.

Course Overview  
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. 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.
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.

Week 1: Introductory Lecture
Week 2: Overview of Encryption Protocols
Week 3: Overview of Authentication Protocols
Week 4: SSL
Week 5: SSL in Detail, TLS, & SET
Week 6: Midterm (Compulsory)
Week 7: 802.11i
Week 8 IPsec
Week 9: IPsec2
Week 10: Intrusion Detection
Week 11: SNMP Security and Mock Exam
Week 12: Review

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, Network Security Essentials, Applications and Standards, 3rd (or 4th) Edition, Publisher: Prentice Hall, 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.

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.

Teaching Methods & Strategies

Lectures, Tutorials and Labs

You are strongly encouraged to attend all class lectures. This is especially the case for this class as you will be presented with brand new concepts that you have likely never come across before. This makes the class very interesting for you – but it does require your participation in class. PDFs of power-points will be 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 power-point presentations, discussion of material in prescribed texts, and potentially, discussion of case studies. You are strongly encouraged to participate in class by interacting through questions and discussions of class material, and to prepare before class by reading relevant work packages ahead of time. There will be plenty of problem sets that will be reviewed during the tutorials. There may be guest lecturers.

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 sniffer (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.

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 Tele 3118. 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

**Assessment Weighting**

- **Final Examination (50%):** The examination is of two-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 a compulsory test. There are zero marks for non-attendance at the mid-term.
- **Laboratory Assessment (30%):** There are six lab tasks, which will be assessed in terms of written reports of lab work, and testing of software developed during labs.
- **Optional Assignment (5%).** An optional assignment is available for students. This provides for up to 5% extra marks beyond normal class marks. More details in class.

**Course Evaluation**

All students will be given the opportunity to provide feedback on the course. You are strongly encouraged to participate in this. Teaching staff take such feedback seriously and use it to improve the course delivery for subsequent lectures.

**Consultations**

If you need additional consultation above and beyond the standard class consultation, please make an appointment via e-mail with the instructor. All email must be from a UNSW student account. Standard consultation time will be announced during week 1.
Other Course Resources.
This course will be conducted using a combination of the course web-site (https://subjects.ee.unsw.edu.au/tele3119) and Moodle (moodle.eng.unsw.edu.au). It is expected and assumed that you will check these online resources at least once per week for important class announcements.

Plagiarism is strictly prohibited.
Please refer to UNSW’s plagiarism policy at http://www.lc.unsw.edu.au/plagiarism/.