FIT5037 Advanced network security - Semester 2, 2013

This unit aims to provide students with an advanced knowledge of network security. Topics to be covered include the design and implementation of some important public key systems: RSA and Elliptic Curve algorithms; concepts of quantum cryptography; quantum computing and cryptography; wireless computing and cryptography; design, implementation and configuration of firewalls in depth; design, implementation and configuration of intrusion detection systems; prevention systems; advanced network security architectures; advanced wireless security: principle and practice; security in trusted-based computing environments; and quantum cryptography.

Mode of Delivery

Caulfield (Day)

Contact Hours

2 hrs lectures/wk, 2 hrs laboratories/wk

Workload requirements

Workload commitments per week are:

Two-hour lecture, two-hour tutorial (or laboratory) requiring preparation in advance, and a minimum of two-hours of personal study per one-hour of contact time in order to satisfy the reading and assignment expectations.

Unit Relationships

Prohibitions

CPE5021

Prerequisites

FIT5044

Chief Examiner

Dr Phu Le

Campus Lecturer

Caulfield

Phu Dung Le

Consultation hours: TBA
Academic Overview

Learning Outcomes

At the completion of this unit students will:

- understand the design and implementation of advanced cryptographic algorithms for wired and wireless computing environments including the design and implementation of RSA and ECC;
- achieve sound knowledge of network security components including the design, implementation, and configuration of Firewalls, Intrusion Detection Systems (static and dynamic checking of programs, anomaly detection, large-scale (Internet-wide) distributed intrusion detection, early sensing, complex attack scenario analysis, and automated response), Prevention Systems, Firewalls, IDSs, VPNs and prevention systems together;
- develop knowledge of advanced network security architectures to allow better network protection, load balancing and recovery from attacks;
- achieve sound knowledge of wireless network security;
- understand security in trusted-based computing environments;
- understand Quantum cryptography.
## Unit Schedule

<table>
<thead>
<tr>
<th>Week</th>
<th>Activities</th>
<th>Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>No formal assessment or activities are undertaken in week 0</td>
</tr>
<tr>
<td>1</td>
<td>Modern computing and network security</td>
<td>Weekly tutorials/Lab Exercises (Week 2 to Week 10) commence</td>
</tr>
<tr>
<td>2</td>
<td>Modern Crypto Systems</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>ECC design and implementation</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Introduction to intrusion detection systems</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Wireless Network Security</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Wireless Network Security (continued)</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Networked and distributed software security</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Networked and distributed software security (continued)</td>
<td>Individual Assignment due Week 8, Friday 4pm</td>
</tr>
<tr>
<td>9</td>
<td>Computer system security and performance</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Security of large computer systems including virtual networks and cloud computing systems</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Advanced theories and network security approaches (if there is still time)</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Theoretical Test in lecture</td>
<td>Theoretical Test in Week 12 lecture</td>
</tr>
<tr>
<td></td>
<td>SWOT VAC</td>
<td>No formal assessment is undertaken in SWOT VAC; Group Assignment due Week 14, Monday 4pm</td>
</tr>
</tbody>
</table>

*Unit Schedule details will be maintained and communicated to you via your learning system.*

## Assessment Summary

Assignments: 40%; Lab exercises and group assignments: 30%; Theoretical test: 30%

<table>
<thead>
<tr>
<th>Assessment Task</th>
<th>Value</th>
<th>Due Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual Assignment</td>
<td>40%</td>
<td>Week 8, Friday 4pm</td>
</tr>
<tr>
<td>Group Assignment</td>
<td>20%</td>
<td>Week 14, Monday 4pm</td>
</tr>
<tr>
<td>Lab Exercises</td>
<td>10%</td>
<td>Weekly (Week 2 to Week 10)</td>
</tr>
<tr>
<td>Theoretical Test</td>
<td>30%</td>
<td>Week 12 lecture</td>
</tr>
</tbody>
</table>
Unit Schedule

Teaching Approach

Lecture and tutorials or problem classes

This teaching and learning approach provides facilitated learning, practical exploration and peer learning.
Assessment Requirements

Assessment Policy

Faculty Policy - Unit Assessment Hurdles

Academic Integrity - Please see the Demystifying Citing and Referencing tutorial at
http://lib.monash.edu/tutorials/citing/

Assessment Tasks

Participation

• Assessment task 1

  Title: Individual Assignment
  Description: Part I: You are required to design and implement the ECC or Lattice Based public key systems using C or C++ or Java.

  Part II: You are required to apply your ECC in 3 network services.

  More details will be provided on the assignment specification.
  Weighting: 40%
  Criteria for assessment: You have to demonstrate your understanding of the algorithms used in your implementation. A good security analysis of your implementation will give you 30% of the total mark. If your code works and reflects the theory of ECC (or lattice-base crypto system) and you can apply it in your three services, this will give you another 30%. Your correct demonstration and answers to interview questions will give you the final 40% of the mark.
  Due date: Week 8, Friday 4pm

• Assessment task 2

  Title: Group Assignment
  Description: You are required to set up, configure and test your complete defence system using using your computers and virtual machines.

  More details will be provided on the assignment specification and lab work sheets.

  For the group assignment, students will receive equal marks, however every member of the group will be interviewed.
  Weighting: 20%
  Criteria for assessment:
If you install and configure all the required system security services correctly you will be given 20% of the total mark. Providing correctly written test plans will give you another 40%. Your demonstration of your tests and answers to interview questions will be worth 40% of the total mark.

Due date:
  Week 14, Monday 4pm

• Assessment task 3

Title:
  Lab Exercises

Description:
  Lab exercises will be handed out each week from Week 2 to Week 10. Please read the handouts for details.

Weighting:
  10%

Criteria for assessment:
  You will get the full mark if you can complete the exercise and demonstrate it. Different marks will be given depending on the level of completion and demonstration.

Due date:
  Weekly (Week 2 to Week 10)

• Assessment task 4

Title:
  Theoretical Test

Description:
  The theoretical test will evaluate your understanding of the theories covered in the unit. It is an open book test and 80% are multiple choice questions and 20% are short answer questions. You will have to study all the materials delivered in the lectures and tutorials/labs.

Weighting:
  30%

Criteria for assessment:
  Correct answers to questions, demonstrating understanding of the materials learned.

Due date:
  Week 12 lecture

Learning resources

Monash Library Unit Reading List
http://readinglists.lib.monash.edu/index.html

Feedback to you

Types of feedback you can expect to receive in this unit are:

• Informal feedback on progress in labs/tutes
Assessment Requirements

**Extensions and penalties**

Submission must be made by the due date otherwise penalties will be enforced.


**Returning assignments**

Students can expect assignments to be returned within two weeks of the submission date or after receipt, whichever is later.

**Assignment submission**

It is a University requirement ([http://www.policy.monash.edu/policy-bank/academic/education/conduct/plagiarism-procedures.html](http://www.policy.monash.edu/policy-bank/academic/education/conduct/plagiarism-procedures.html)) for students to submit an assignment coversheet for each assessment item. Faculty Assignment coversheets can be found at [http://www.infotech.monash.edu.au/resources/student/forms/](http://www.infotech.monash.edu.au/resources/student/forms/). Please check with your Lecturer on the submission method for your assignment coversheet (e.g. attach a file to the online assignment submission, hand-in a hard copy, or use an online quiz). Please note that it is your responsibility to retain copies of your assessments.

**Online submission**

If Electronic Submission has been approved for your unit, please submit your work via the learning system for this unit, which you can access via links in the my.monash portal.

**Required Resources**

Please check with your lecturer before purchasing any Required Resources. Limited copies of prescribed texts are available for you to borrow in the library, and prescribed software is available in student labs.

Removable hard drives and Scientific Linux software will be provided at the labs.
Other Information

Policies

Monash has educational policies, procedures and guidelines, which are designed to ensure that staff and students are aware of the University’s academic standards, and to provide advice on how they might uphold them. You can find Monash’s Education Policies at:

Key educational policies include:

- Academic integrity:
  http://www.policy.monash.edu/policy-bank/academic/education/conduct/student-academic-integrity-policy.html
- Assessment in Coursework Programs;
- Special Consideration;
  http://www.policy.monash.edu/policy-bank/academic/education/assessment/special-consideration-policy.html
- Grading Scale;
  http://www.policy.monash.edu/policy-bank/academic/education/assessment/grading-scale-policy.html
- Discipline: Student Policy;
  http://www.policy.monash.edu/policy-bank/academic/education/conduct/student-discipline-policy.html
- Academic Calendar and Semesters; http://www.monash.edu.au/students/dates/
- Orientation and Transition; http://intranet.monash.edu.au/infotech/resources/students/orientation/
- Academic and Administrative Complaints and Grievances Policy;
  http://www.policy.monash.edu/policy-bank/academic/education/management/complaints-grievance-policy.html
- Code of Practice for Teaching and Learning;
- Graduate Attributes Policy
  http://www.policy.monash.edu/policy-bank/academic/education/management/monash-graduate-attributes-policy.html

Student services

The University provides many different kinds of support services for you. Contact your tutor if you need advice and see the range of services available at http://www.monash.edu.au/students. For Sunway see http://www.monash.edu.my/Student-services, and for South Africa see http://www.monash.ac.za/current/.

Monash University Library

The Monash University Library provides a range of services, resources and programs that enable you to save time and be more effective in your learning and research. Go to www.lib.monash.edu.au or the library tab in my.monash portal for more information. At Sunway, visit the Library and Learning Commons at http://www.lib.monash.edu.my/. At South Africa visit http://www.lib.monash.ac.za/.
Disability Liaison Unit

Students who have a disability or medical condition are welcome to contact the Disability Liaison Unit to discuss academic support services. Disability Liaison Officers (DLOs) visit all Victorian campuses on a regular basis.

Website: http://www.monash.edu/equity-diversity/disability/index.html
Telephone: 03 9905 5704 to book an appointment with a DLO; or contact the Student Advisor, Student Community Services at 03 55146018 at Sunway
Email: dlu@monash.edu
Drop In: Equity and Diversity Centre, Level 1, Building 55, Clayton Campus, or Student Community Services Department, Level 2, Building 2, Monash University, Sunway Campus

Your feedback to Us

Monash is committed to excellence in education and regularly seeks feedback from students, employers and staff. One of the key formal ways students have to provide feedback is through the Student Evaluation of Teaching and Units (SETU) survey. The University’s student evaluation policy requires that every unit is evaluated each year. Students are strongly encouraged to complete the surveys. The feedback is anonymous and provides the Faculty with evidence of aspects that students are satisfied and areas for improvement.

For more information on Monash’s educational strategy, see:
www.monash.edu.au/about/monash-directions and on student evaluations, see:
www.policy.monash.edu/policy-bank/academic/education/quality/student-evaluation-policy.html

Previous Student Evaluations of this Unit

Feedback from past students clearly has highlighted the following strengths and necessary improvements:

1. The unit has advanced students in the area of network security and it was a plus to their degree.
2. Assignments tasks were too difficult for some students, especially the implementations of RSA and ECC.
3. Assignments tasks required too much of reading and research.

If you wish to view how previous students rated this unit, please go to