COMP8310
Security Technologies and Forensic Analysis
Session 1, Weekday attendance, North Ryde 2020
Dept of Computing

Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Information</td>
<td>2</td>
</tr>
<tr>
<td>Learning Outcomes</td>
<td>2</td>
</tr>
<tr>
<td>General Assessment Information</td>
<td>3</td>
</tr>
<tr>
<td>Assessment Tasks</td>
<td>3</td>
</tr>
<tr>
<td>Delivery and Resources</td>
<td>6</td>
</tr>
<tr>
<td>Unit Schedule</td>
<td>7</td>
</tr>
<tr>
<td>Policies and Procedures</td>
<td>9</td>
</tr>
</tbody>
</table>

Disclaimer
Macquarie University has taken all reasonable measures to ensure the information in this publication is accurate and up-to-date. However, the information may change or become out-dated as a result of change in University policies, procedures or rules. The University reserves the right to make changes to any information in this publication without notice. Users of this publication are advised to check the website version of this publication [or the relevant faculty or department] before acting on any information in this publication.
General Information

Unit convenor and teaching staff
Milton Baar
milton.baar@mq.edu.au
Contact via 04 1927 9847
By arrangement on the day of the lecture delivery

Credit points
10

Prerequisites
ITEC647 or COMP6250

Corequisites

Co-badged status

Unit description
This unit covers the fundamental technologies and processes that underpin good systems security management within modern organisations. We consider the underlying mechanics of information and communications technology security infrastructures, risk management, attack modelling, software security, firewalls, intrusion detection and forensics.

Important Academic Dates
Information about important academic dates including deadlines for withdrawing from units are available at https://students.mq.edu.au/important-dates

Learning Outcomes

ULO1: Analyse the key security requirements and trends in software security and interconnected systems. Identify key threats and analysis tools to evaluate security deficiencies.

ULO2: Analyse techniques for exploiting software and networks. Investigate operating system and file system platforms and identify attack surface.

ULO3: Design and/or apply security techniques to mitigate software and network attacks. Identification of tools and recovery mechanisms, including forensic analysis and process.

ULO4: Evaluate security techniques used to deal with the attacks and the limitations of forensic tools.
ULO5: Present and discuss concepts related to software and network security at an advanced level.

General Assessment Information

Late Submission

No extensions will be granted without an approved application for Special Consideration. There will be a deduction of 10% of the total available marks made from the total awarded mark for each 24 hour period or part thereof that the submission is late. For example, 25 hours late in submission for an assignment worth 10 marks – 20% penalty or 2 marks deducted from the total. No submission will be accepted after solutions have been posted.

Hurdle assessments:

- Students must achieve at least 20/40 in the final exam to be eligible to pass the unit.
- A second attempt will be provided for students that achieve a mark in the band 15/40 to 19.9/40 in the final exam.
- Students must achieve at least 15/20 in the practical lab reports to be eligible to pass the unit.
- An additional practical assessment task will be provided for students that achieve a mark in the band 10/20 to 14.9/20 in the practical lab report.

If you apply for Special Consideration for your final examination, you must make yourself available for the week after the completion of postgraduate exams. If you are not available at that time, there is no guarantee an additional examination time will be offered. Specific examination dates and times will be determined at a later date.

Second-chance hurdle examinations will also be offered in the week after the completion of postgraduate exams. You will be notified of your eligibility for a hurdle retry and you must also make yourself available during that week to take advantage of this opportunity.

Assessment Tasks

<table>
<thead>
<tr>
<th>Name</th>
<th>Weighting</th>
<th>Hurdle</th>
<th>Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>Practical activities report</td>
<td>20%</td>
<td>Yes</td>
<td>Week 13</td>
</tr>
<tr>
<td>Final Examination</td>
<td>40%</td>
<td>Yes</td>
<td>During the examination period</td>
</tr>
<tr>
<td>Quiz 1</td>
<td>5%</td>
<td>No</td>
<td>Week 5</td>
</tr>
<tr>
<td>Group Project</td>
<td>30%</td>
<td>No</td>
<td>Weeks 11 &amp; 12</td>
</tr>
<tr>
<td>Quiz 2</td>
<td>5%</td>
<td>No</td>
<td>Week 9</td>
</tr>
</tbody>
</table>
Practical activities report

Assessment Type 1: Report
Indicative Time on Task 2: 10 hours
Due: Week 13
Weighting: 20%
This is a hurdle assessment task (see assessment policy for more information on hurdle assessment tasks)

During the unit, there will be practical activities relating to security technologies and forensics.

On successful completion you will be able to:

• Analyse techniques for exploiting software and networks. Investigate operating system and file system platforms and identify attack surface.
• Design and/or apply security techniques to mitigate software and network attacks. Identification of tools and recovery mechanisms, including forensic analysis and process.
• Evaluate security techniques used to deal with the attacks and the limitations of forensic tools.
• Present and discuss concepts related to software and network security at an advanced level.

Final Examination

Assessment Type 1: Examination
Indicative Time on Task 2: 20 hours
Due: During the examination period
Weighting: 40%
This is a hurdle assessment task (see assessment policy for more information on hurdle assessment tasks)

The exam will be a written exam with questions from topics covered in the lectures. It will be held in the usual examination period of the semester. Students have 2 hours written time plus 10 minutes reading time for the exam.

On successful completion you will be able to:

• Analyse the key security requirements and trends in software security and interconnected systems. Identify key threats and analysis tools to evaluate security deficiencies.
• Analyse techniques for exploiting software and networks. Investigate operating system and file system platforms and identify attack surface.
• Design and/or apply security techniques to mitigate software and network attacks.
Identification of tools and recovery mechanisms, including forensic analysis and process.
- Evaluate security techniques used to deal with the attacks and the limitations of forensic tools.

Quiz 1
Assessment Type 1: Quiz/Test
Indicative Time on Task 2: 2 hours
Due: Week 5
Weighting: 5%

This quiz (closed book) will be based on your previously covered lecture material for weeks 1-4. The quiz questions will be online multiple choice. Quiz will serve as a feedback mechanism to monitor your progress in the unit and there will be a discussion on the solutions when all students have completed the quiz.

On successful completion you will be able to:
- Analyse the key security requirements and trends in software security and interconnected systems. Identify key threats and analysis tools to evaluate security deficiencies.
- Analyse techniques for exploiting software and networks. Investigate operating system and file system platforms and identify attack surface.

Group Project
Assessment Type 1: Project
Indicative Time on Task 2: 15 hours
Due: Weeks 11 & 12
Weighting: 30%

Presentations are held in weeks 11 & 12 but content due by mid semester. Group project with 3-4 students per group. Projects will be related to security and forensics issues with emerging technologies such as smart grid and cloud.

Each group will be allocated a time slot for presenting their work during Week 11 OR Week 12. Each student in the group is expected to present their work which will be followed by QA session. The QA session will be conducted by the panel (which includes convener and/or other staff members and/or PhD students within the computing department).

The presentation and QA session will help the panel to evaluate the individual contribution of each student.

The Project will account to 30% (Report-10%, Presentation-10% and QA-10%) of the unit marks.

On successful completion you will be able to:
- Analyse the key security requirements and trends in software security and
interconnected systems. Identify key threats and analysis tools to evaluate security deficiencies.

- Analyse techniques for exploiting software and networks. Investigate operating system and file system platforms and identify attack surface.
- Design and/or apply security techniques to mitigate software and network attacks. Identification of tools and recovery mechanisms, including forensic analysis and process.
- Evaluate security techniques used to deal with the attacks and the limitations of forensic tools.
- Present and discuss concepts related to software and network security at an advanced level.

**Quiz 2**

**Assessment Type:** Quiz/Test  
**Indicative Time on Task:** 3 hours  
**Due:** Week 9  
**Weighting:** 5%

This quiz (closed book) will be based on your previously covered lecture material for weeks 5-8. The quiz questions will be short answer. Quiz will serve as a feedback mechanism to monitor your progress in the unit and there will be a discussion on the solutions when all students have completed the quiz.

On successful completion you will be able to:

- Analyse the key security requirements and trends in software security and interconnected systems. Identify key threats and analysis tools to evaluate security deficiencies.
- Analyse techniques for exploiting software and networks. Investigate operating system and file system platforms and identify attack surface.

---

1 If you need guidance or support to understand or complete this type of assessment, please contact the Learning Skills Team

2 Indicative time-on-task is an estimate of the time required for completion of the assessment task and is subject to individual variation

**Delivery and Resources**

This unit covers the fundamental technologies and processes that underpin good systems security management within modern organisations. We consider the underlying mechanics of information technology security infrastructures, risk management, attack modelling, software security, and forensics.
1. Students may undertake some practical activities in the Computing Lab(s). However, students will have a better learning experience if they provide their own laptop (Mac or Windows) that they can use when Lab access is unavailable.

2. Major assessment tasks are based on practical tasks, and these tasks may be started in the Labs but require more time that there is available in the Labs. These are considered "take home tasks".

## Unit Schedule

### Unit Schedule

To successfully participate in the lab exercises and to understand the fundamentals of this unit, students should read and view the material at the following links before week 4.

**Watch these:**

- Binary/octal/decimal/hexadecimal number systems, [https://www.youtube.com/watch?v=5sS7w-CMHkU](https://www.youtube.com/watch?v=5sS7w-CMHkU)
- Endian concepts, [https://www.youtube.com/watch?v=NvlSRs_APT4](https://www.youtube.com/watch?v=NvlSRs_APT4)
- ASCII/EBCDIC/Unicode concepts, [https://www.youtube.com/watch?v=m0aOZulMhhhE](https://www.youtube.com/watch?v=m0aOZulMhhhE)
- Boot process, [https://www.youtube.com/watch?v=P-zWXbPh_dg](https://www.youtube.com/watch?v=P-zWXbPh_dg)
- Operating system and kernel architecture, [https://www.youtube.com/watch?v=9GDX-lyZ_C8](https://www.youtube.com/watch?v=9GDX-lyZ_C8)
- Protection ring, [https://www.youtube.com/watch?v=b3HlH4IubZE](https://www.youtube.com/watch?v=b3HlH4IubZE)

**Read these:**

- Introduction to operating systems, [https://www.cs.uic.edu/~jbell/CourseNotes/OperatingSystems/1_Introduction.html](https://www.cs.uic.edu/~jbell/CourseNotes/OperatingSystems/1_Introduction.html)

<table>
<thead>
<tr>
<th>Week</th>
<th>Topic</th>
<th>Lab/Practical activity</th>
<th>Recommended reading and/or viewing</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction</td>
<td>No week 1 lab</td>
<td></td>
</tr>
<tr>
<td>Week</td>
<td>Topic</td>
<td>Lab/Practical activity</td>
<td>Recommended reading and/or viewing</td>
</tr>
<tr>
<td>------</td>
<td>------------------------------</td>
<td>------------------------</td>
<td>-----------------------------------</td>
</tr>
</tbody>
</table>
| 2    | Risk management frameworks  | Lab systems setup      | • Overview of Digital Forensics, [https://www.youtube.com/watch?v=ZUqzcQc_syE](https://www.youtube.com/watch?v=ZUqzcQc_syE)  
• Digital Forensics TEDx presentation, [https://www.youtube.com/watch?v=PF-JnQIAEew](https://www.youtube.com/watch?v=PF-JnQIAEew) |
| 3    | Operating systems vulnerabilities | Forensic tools part 1 |                                   |
| 4    | Introduction to file systems |                        | • Windows File System Structures, [https://www.youtube.com/watch?v=atYQBTHhnyY](https://www.youtube.com/watch?v=atYQBTHhnyY)  
• FAT file system explained, [https://www.youtube.com/watch?v=HjVktRd35G8](https://www.youtube.com/watch?v=HjVktRd35G8)  
• Windows ReFS Explained, [https://www.youtube.com/watch?v=L9kNND7b9yw](https://www.youtube.com/watch?v=L9kNND7b9yw)  
• ReFS in Windows Server 2012, [https://www.youtube.com/watch?v=WWeZF94gXZs](https://www.youtube.com/watch?v=WWeZF94gXZs)  
| 5    | Linux file systems          | Quiz 1                  | Difference Between Linux and Windows, [https://www.youtube.com/watch?v=NXZoWJVOhXI](https://www.youtube.com/watch?v=NXZoWJVOhXI) |
| 6    | Introduction to Digital Evidence and Computer Crime | Forensic management tools |                                   |
| 7    | "Big end of town" file systems | Experimentation when tools fail you |                                   |
| 8    | Mid-course review           | Guest Speaker           |                                   |
| 9    | Steganography               | Quiz 2                  | Steganography lab                |
| 10   | Introduction to cryptography | Practical lab report writing |                                   |
| 11   | Group project presentation  |                        |                                   |
| 12   | Group project presentation  |                        |                                   |
Policies and Procedures

Macquarie University policies and procedures are accessible from Policy Central (https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policy-central). Students should be aware of the following policies in particular with regard to Learning and Teaching:

- Academic Appeals Policy
- Academic Integrity Policy
- Academic Progression Policy
- Assessment Policy
- Fitness to Practice Procedure
- Grade Appeal Policy
- Complaint Management Procedure for Students and Members of the Public
- Special Consideration Policy (Note: The Special Consideration Policy is effective from 4 December 2017 and replaces the Disruption to Studies Policy.)

Students seeking more policy resources can visit the Student Policy Gateway (https://students.mq.edu.au/support/study/student-policy-gateway). It is your one-stop-shop for the key policies you need to know about throughout your undergraduate student journey.

If you would like to see all the policies relevant to Learning and Teaching visit Policy Central (https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policy-central).

Student Code of Conduct

Macquarie University students have a responsibility to be familiar with the Student Code of Conduct: https://students.mq.edu.au/study/getting-started/student-conduct

Results

Results published on platform other than eStudent, (eg. iLearn, Coursera etc.) or released directly by your Unit Convenor, are not confirmed as they are subject to final approval by the University. Once approved, final results will be sent to your student email address and will be made available in eStudent. For more information visit ask.mq.edu.au or if you are a Global MBA student contact globalmba.support@mq.edu.au
Student Support
Macquarie University provides a range of support services for students. For details, visit http://students.mq.edu.au/support/

Learning Skills
Learning Skills (mq.edu.au/learningskills) provides academic writing resources and study strategies to improve your marks and take control of your study.

- Workshops
- StudyWise
- Academic Integrity Module for Students
- Ask a Learning Adviser

Student Enquiry Service
For all student enquiries, visit Student Connect at ask.mq.edu.au

If you are a Global MBA student contact globalmba.support@mq.edu.au

Equity Support
Students with a disability are encouraged to contact the Disability Service who can provide appropriate help with any issues that arise during their studies.

IT Help
For help with University computer systems and technology, visit http://www.mq.edu.au/about_us/offices_and_units/information_technology/help/.

When using the University’s IT, you must adhere to the Acceptable Use of IT Resources Policy. The policy applies to all who connect to the MQ network including students.