COMP8310

Security Technologies and Forensic Analysis

Session 1, Weekday attendance, North Ryde 2020

Department of Computing

Contents

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

On successful completion of this unit, you will be able to:

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.

Assessment Tasks

Coronavirus (COVID-19) Update

Assessment details are no longer provided here as a result of changes due to the Coronavirus (COVID-19) pandemic.

Students should consult iLearn for revised unit information.

Find out more about the Coronavirus (COVID-19) and potential impacts on staff and students

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.

Delivery and Resources

Coronavirus (COVID-19) Update

Any references to on-campus delivery below may no longer be relevant due to COVID-19.

Please check here for updated delivery information: https://ask.mq.edu.au/account/pub/display/unit_status

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 in 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

Coronavirus (COVID-19) Update

The unit schedule/topics and any references to on-campus delivery below may no longer be relevant due to COVID-19. Please consult iLearn for latest details, and check here for updated delivery information: https://ask.mq.edu.au/account/pub/display/unit_status

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
- Endian concepts, https://www.youtube.com/watch?v=NvISRs_APT4
- ASCII/EBCDIC/Unicode concepts, https://www.youtube.com/watch?v=m0aOZuMhhhE
- Boot process, https://www.youtube.com/watch?v=P-zWXbPh_dg
- Operating system and kernel architecture, https://www.youtube.com/watch?v=9GDX-IyZ_C8

- Protection ring, https://www.youtube.com/watch?v=b3HlH4IubZE

Read these:

- Introduction to operating systems, https://www.cs.uic.edu/~jbell/CourseNotes/OperatingSystems/1_Introduction.html
- Forensic analysis of smart TV: A current issue and call to arms, http://www.sciencedirect.com/science/article/pii/S1742287614000620
- How computers measure and keep time, https://www.eecis.udel.edu/~ntp/ntpfaq/NTP-s-sw-clocks.htm

Week	Topic	Lab/ Practical activity	Recommended reading and/or viewing
1	Introduction	No week 1 lab	
2	Risk management frameworks	Lab systems setup	• Overview of Digital Forensics, https://www.youtube.com/watch?v=ZUqzcQc_syE • Digital Forensics TEDx presentation, https://www.youtube.com/watch?v=Pf-JnQfAEew
3	Operating systems vulnerabilities	Forensic tools part 1	
4	Introduction to file systems		• Windows File System Structures, https://www.youtube.com/watch?v=atYQBTHnjyY • FAT file system explained, https://www.youtube.com/watch?v=HjVktRd35G8 • Windows ReFS Explained, https://www.youtube.com/watch?v=L9kNND7b9yw • ReFS in Windows Server 2012, https://www.youtube.com/watch?v=WWeZf94gXZs • Windows filesystems, https://support.microsoft.com/en-us/help/100108/overview-of-fat--hpfs--and-ntfs-file-systems • Recovering Deleted and Wiped Files: A Digital Forensic Comparison of FAT32 and NTFS File Systems using Evidence Eliminator, http://www.swdsi.org/swdsi2010/sw2010_preceedings/papers/pa121.pdf
5	Linux file systems	Quiz 1 Investigating Linux	Difference Between Linux and Windows, https://www.youtube.com/watch?v=NXZoWJVOhXI
6	Introduction to Digital Evidence and Computer Crime	Forensic management tools	

Week	Topic	Lab/ Practical activity	Recommended reading and/or viewing
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		
13	Review		

*Lecture contents, order and schedule of lectures and practicals will vary depending on the class progress.

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 help you improve your marks and take control of your study.

- Getting help with your assignment
- Workshops
- StudyWise
- Academic Integrity Module

The Library provides online and face to face support to help you find and use relevant information resources.

- Subject and Research Guides
- Ask a Librarian

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.