COIT20262 *Advanced Network Security*
Term 2 - 2018

Profile information current as at 26/04/2024 04:39 am

General Information

Overview

In this unit, you will learn how to protect the confidentiality, integrity and availability of information and network services in business organisations. You will study the fundamental cryptographic techniques that many of the security mechanisms are built upon. You will also study network security attacks, including malware, denial of service, and application vulnerabilities, and the corresponding countermeasures. Through computer laboratory activities, you will gain hands-on experience in analysing attacks and deploying defences, including securing web applications, establishing access control mechanisms, and applying encryption in wired and wireless networks.

Details

Career Level: *Postgraduate*
Unit Level: *Level 9*
Credit Points: *6*
Student Contribution Band: *8*
Fraction of Full-Time Student Load: *0.125*

Pre-requisites or Co-requisites

Prerequisite: COIT20261 Network Routing and Switching
Important note: Students enrolled in a subsequent unit who failed their pre-requisite unit, should drop the subsequent unit before the census date or within 10 working days of Fail grade notification. Students who do not drop the unit in this timeframe cannot later drop the unit without academic and financial liability. See details in the Assessment Policy and Procedure (Higher Education Coursework).

Offerings For Term 2 - 2018

- Brisbane
- Distance
- Melbourne
- Rockhampton
- Sydney

Attendance Requirements

All on-campus students are expected to attend scheduled classes – in some units, these classes are identified as a mandatory (pass/fail) component and attendance is compulsory. International students, on a student visa, must maintain a full time study load and meet both attendance and academic progress requirements in each study period (satisfactory attendance for International students is defined as maintaining at least an 80% attendance record).

Website

This unit has a website, within the Moodle system, which is available two weeks before the start of term. It is important that you visit your Moodle site throughout the term. Please visit Moodle for more information.

Class and Assessment Overview

Recommended Student Time Commitment

Each 6-credit Postgraduate unit at CQUniversity requires an overall time commitment of an average of 12.5 hours of study per week, making a total of 150 hours for the unit.

Class Timetable

Regional Campuses
Bundaberg, Cairns, Emerald, Gladstone, Mackay, Rockhampton, Townsville

Metropolitan Campuses
Adelaide, Brisbane, Melbourne, Perth, Sydney

Assessment Overview

1. **Written Assessment**
Weighting: 40%
2. **Written Assessment**
Weighting: 45%
3. **Online Quiz(zes)**
Weighting: 15%

Assessment Grading

This is a graded unit: your overall grade will be calculated from the marks or grades for each assessment task, based on the relative weightings shown in the table above. You must obtain an overall mark for the unit of at least 50%, or an overall grade of 'pass' in order to pass the unit. If any 'pass/fail' tasks are shown in the table above they must also be completed successfully ('pass' grade). You must also meet any minimum mark requirements specified for a particular assessment task, as detailed in the 'assessment task' section (note that in some instances, the minimum mark for a task may be greater than 50%). Consult the University's Grades and Results Policy for more details of interim results and final grades.

CQUniversity Policies

All University policies are available on the CQUniversity Policy site.
You may wish to view these policies:

- Grades and Results Policy
- Assessment Policy and Procedure (Higher Education Coursework)
- Review of Grade Procedure
- Student Academic Integrity Policy and Procedure
- Monitoring Academic Progress (MAP) Policy and Procedure – Domestic Students
- Monitoring Academic Progress (MAP) Policy and Procedure – International Students
- Student Refund and Credit Balance Policy and Procedure
- Student Feedback – Compliments and Complaints Policy and Procedure
- Information and Communications Technology Acceptable Use Policy and Procedure

This list is not an exhaustive list of all University policies. The full list of University policies are available on the CQUniversity Policy site.

Previous Student Feedback

Feedback, Recommendations and Responses

Every unit is reviewed for enhancement each year. At the most recent review, the following staff and student feedback items were identified and recommendations were made.

Feedback from Student emails.

Feedback
Software was difficult to use on a Mac, as the instructions were out of date for the latest Mac version.

Recommendation
Update the software instructions for the latest operating systems, while also making it clear that Windows is the only environment supported by teaching team (as the computer labs only have Windows).

Feedback from Teaching team, student feedback.

Feedback
Workshop tasks in first few weeks are too time consuming or complex.

Recommendation
The early workshop tasks are important for understanding later tasks. Lecture content should be reduced so that some more time can be spent explaining the workshop tasks.

Feedback from Teaching team, Self-reflection.

Feedback
Customised online textbook is hard to access and is getting out of date.

Recommendation
Review options for a new textbook, either a different book or another customised online textbook that uses new versions.

Unit Learning Outcomes

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

1. Explain vulnerabilities and attacks, as well as their countermeasures
2. Use and compare cryptographic techniques for securing computers and networks
3. Design security controls for organisations, such as firewalls, authentication, and access control
4. Develop and deploy network security technologies, including encryption software, VPNs and wireless security
5. Assess emerging threats and security controls.

Australian Computer Society (ACS) recognises the Skills Framework for the Information Age (SFIA). SFIA is in use in over 100 countries and provides a widely used and consistent definition of ICT skills. SFIA is increasingly being used when developing job descriptions and role profiles.
ACS members can use the tool MySFIA to build a skills profile at
https://www.acs.org.au/professionalrecognition/mysfia-b2c.html
This unit contributes to the following workplace skills as defined by SFIA. The SFIA code is included:

- Information Security (SCTY)
- Security Administration (SCAD)
- Information Assurance (INAS)
- Technical Specialism (TECH)
- Consultancy (CNSL)
- IT Governance (GOVN)

Alignment of Learning Outcomes, Assessment and Graduate Attributes

— N/A Level | • Introductory Level | • Intermediate Level | • Graduate Level | ◦ Professional Level | ◦ Advanced Level

Alignment of Assessment Tasks to Learning Outcomes

Assessment Tasks	Learning Outcomes				
	1	2	3	4	5
1 - Written Assessment - 40%	•	•			•
2 - Online Quiz(zes) - 15%	•	•	•	•	
3 - Written Assessment - 45%			•	•	•

Alignment of Graduate Attributes to Learning Outcomes

Graduate Attributes	Learning Outcomes				
	1	2	3	4	5
1 - Knowledge	◦	◦	◦	◦	◦
2 - Communication	◦	◦	◦	◦	◦
3 - Cognitive, technical and creative skills	◦	◦	◦	◦	◦
4 - Research		◦			◦
5 - Self-management		◦		◦	◦
6 - Ethical and Professional Responsibility	◦	◦	◦	◦	◦
7 - Leadership					
8 - Aboriginal and Torres Strait Islander Cultures					

Alignment of Assessment Tasks to Graduate Attributes

Assessment Tasks	Graduate Attributes							
	1	2	3	4	5	6	7	8
1 - Written Assessment - 40%	◦	◦	◦	◦	◦	◦		
2 - Online Quiz(zes) - 15%	◦	◦	◦	◦	◦	◦		
3 - Written Assessment - 45%	◦	◦	◦	◦	◦	◦		

Textbooks and Resources

Textbooks

COIT20262

Prescribed

Guide to Firewall & VPNs
Edition: 3rd (2012)
Authors: Michael E. Whitman, Herbert J. Mattord, Andrew Green
Cengage Learning
Boston , USA
Binding: Paperback
COIT20262

Prescribed

Guide to Network Defense and Countermeasures
Edition: 3rd (2013)
Authors: Randy Weaver, Dawn Weaver and Dean Farwood
Cengage Learning
Boston , USA
Binding: Paperback
COIT20262

Prescribed

Security + Guide to Network Security Fundamentals
Edition: 5th (2014)
Authors: Mark Ciampa
Cengage Learning
Boston , USA
Binding: Paperback

Additional Textbook Information
A special e-book containing relevant chapters from each of the three textbooks for this course is available from the publisher at:
https://www.cengagebrain.com.au/shop/en/AU/storefront/australia?cmd=CLHeaderSearch&fieldValue=CP1069
Purchase this e-book instead of the three individual textbooks.

IT Resources

You will need access to the following IT resources:

- CQUniversity Student Email
- Internet
- Unit Website (Moodle)
- VirtualBox
- WinSCP or FileZilla
- Wireshark
- Microsoft Windows on CQU Lab computer and/or personal computer

Referencing Style

All submissions for this unit must use the referencing style: Harvard (author-date)
For further information, see the Assessment Tasks.

Teaching Contacts

Steven Gordon Unit Coordinator
s.d.gordon@cqu.edu.au

Schedule

Week 1 - 09 Jul 2018

Module/Topic	Chapter	Events and Submissions/Topic
Introduction to Network Security	Ciampa: Chapter 1	

Week 2 - 16 Jul 2018

Module/Topic	Chapter	Events and Submissions/Topic
Malware and Network Attacks	Ciampa: Chapters 2 & 3	

Week 3 - 23 Jul 2018

Module/Topic	Chapter	Events and Submissions/Topic
Vulnerabilities	Ciampa: Chapters 15 & 4	

Week 4 - 30 Jul 2018

Module/Topic	Chapter	Events and Submissions/Topic
Cryptography	Ciampa: Chapter 5	Quiz 1 due 10am Monday

Week 5 - 06 Aug 2018

Module/Topic	Chapter	Events and Submissions/Topic
Introduction to Firewalls	Whitman: Chapters 4 & 5	

Vacation Week - 13 Aug 2018

Module/Topic	Chapter	Events and Submissions/Topic

Week 6 - 20 Aug 2018

Module/Topic	Chapter	Events and Submissions/Topic
Firewalls and Proxies	Whitman: Chapters 6 & 7	Quiz 2 due 10am Monday **Assignment 1** Due: Week 6 Friday (24 Aug 2018) 5:00 pm AEST

Week 7 - 27 Aug 2018

Module/Topic	Chapter	Events and Submissions/Topic
Authentication	Ciampa: Chapter 12	

Week 8 - 03 Sep 2018

Module/Topic	Chapter	Events and Submissions/Topic
Access Control	Ciampa: Chapter 11	Quiz 3 due 10am Monday

Week 9 - 10 Sep 2018

Module/Topic	Chapter	Events and Submissions/Topic
Internet Security	Ciampa: Chapter 12; Weaver: Chapter 12	

Week 10 - 17 Sep 2018

Module/Topic	Chapter	Events and Submissions/Topic
Virtual Private Networks	Weaver: Chapter 11; Whitman: Chapter 10	Quiz 4 due 10am Monday

Week 11 - 24 Sep 2018

Module/Topic	Chapter	Events and Submissions/Topic
Wireless Network Security	Ciampa: Chapter 9	

Week 12 - 01 Oct 2018

Module/Topic	Chapter	Events and Submissions/Topic

Review and Assignment Completion	-	Quiz 5 due 10am Tuesday (due to public holiday on Monday) **Assignment 2** Due: Week 12 Friday (5 Oct 2018) 5:00 pm AEST

Assessment Tasks

1 Assignment 1

Assessment Type
Written Assessment

Task Description
This assignment requires you to apply knowledge from the lectures and workshops to solve practical problems, as well as to explore new topics not covered in detail in lectures. You will: use software to observe communications across a network, and applying the knowledge to identify security issues and/or design security mechanisms; study and apply cryptographic tools; research and report on state-of-the-art security malware, vulnerabilities and attacks, and possible countermeasures. There will be multiple questions on different topics, and you will be expected to submit a report containing answers to all the questions. The report may be a mix of short answers, diagrams, tables, and short essays with references. In addition to the report, you may be required to submit files produced as output from relevant network security software.
This assignment is individual assessment, and while discussion of questions is encouraged, you must develop and write your own answers, and complete any software tasks on your own. Questions, and expected structure/format of the report, can be found on Moodle.

Assessment Due Date
Week 6 Friday (24 Aug 2018) 5:00 pm AEST

Return Date to Students
Week 8 Friday (7 Sept 2018)

Weighting
40%

Assessment Criteria
The assignment consists of multiple questions, each marked separately. In general, to obtain full marks the answer must be correct, and when an explanation is required, the answer must demonstrate understanding of the problem, solution and tradeoffs.
When additional files are required to be submitted (e.g. output from software), those files must be in the correct format, including with specified filename, and contain content demonstrating that you have correctly performed the task associated with the question. Failure to submit a required file, submission of a file in the incorrect format, or submission of a file that is effectively the same as another student's (when independently performing the tasks would not normally produce the same output), will result in all answers dependent on that file receiving 0 marks.
Mark allocation for each question, the expected format of the answer and any additional files, and details of the marking criteria can be found in the assignment on Moodle.

Referencing Style

- Harvard (author-date)

Submission
Online

Learning Outcomes Assessed

- Explain vulnerabilities and attacks, as well as their countermeasures
- Use and compare cryptographic techniques for securing computers and networks
- Assess emerging threats and security controls.

Graduate Attributes

- Knowledge
- Communication
- Cognitive, technical and creative skills
- Research
- Self-management

- Ethical and Professional Responsibility

2 Assignment 2

Assessment Type
Written Assessment

Task Description
This assignment requires you to apply knowledge from the lectures and workshops to solve practical problems, as well as to explore new topics not covered in detail in lectures. You will: use software to identify and defend against security attacks in network communications; design and implement network and computer access control and authentication mechanisms; and identify problems and design solutions for securing communications in a private/public network. There will be multiple questions on different topics, and you will be expected to submit a report containing answers to all the questions. The report may be a mix of short answers, diagrams, tables, and short essays with references. In addition to the report, you may be required to submit files produced as output from relevant network security software.
This assignment is individual assessment, and while discussion of questions is encouraged, you must develop and write your own answers, and complete any software tasks on your own. Questions, and expected structure/format of the report, can be found on Moodle.

Assessment Due Date
Week 12 Friday (5 Oct 2018) 5:00 pm AEST

Return Date to Students

Certification of Grades day

Weighting
45%

Assessment Criteria
The assignment consists of multiple questions, each marked separately. In general, to obtain full marks the answer must be correct, and when an explanation is required, the answer must demonstrate understanding of the problem, solution and tradeoffs.
When additional files are required to be submitted (e.g. output from software), those files must be in the correct format, including with specified filename, and contain content demonstrating that you have correctly performed the task associated with the question. Failure to submit a required file, submission of a file in the incorrect format, or submission of a file that is effectively the same as another student's (when independently performing the tasks would not normally produce the same output), will result in all answers dependent on that file receiving 0 marks.
Mark allocation for each question, the expected format of the answer and any additional files, and details of the marking criteria can be found in the assignment on Moodle.

Referencing Style

- Harvard (author-date)

Submission
Online

Learning Outcomes Assessed

- Design security controls for organisations, such as firewalls, authentication, and access control
- Develop and deploy network security technologies, including encryption software, VPNs and wireless security
- Assess emerging threats and security controls.

Graduate Attributes

- Knowledge
- Communication
- Cognitive, technical and creative skills
- Research
- Self-management
- Ethical and Professional Responsibility

3 Quizzes

Assessment Type
Online Quiz(zes)

Task Description
You will undertake 5 quizzes on Moodle throughout the term. Each quiz will cover lecture and workshop topics from the

weeks leading up to that quiz, and will not cover topics from the previous quizzes (although some general unit knowledge may be necessary).
The quiz will consist of multiple choice questions, short answer questions and/or calculations. There will be multiple independent questions in each quiz.
Each quiz will be available for approximately 1 week before the due date. The quiz will be time limited and you will be allowed multiple attempts (at least 2), with your highest score counting towards your grade. The time limit and the number of attempts allowed may vary among the quizzes, but will typically be between 15 and 45 minutes and 2 or 3 attempts.
Quizzes are individual assessments, and while they are open book, you are expected to complete the quiz on your own, without the assistance of others. Quiz time limits, topics, attempts allowed and open/close times can be found on Moodle.

Number of Quizzes
5

Frequency of Quizzes
Other

Assessment Due Date

Monday 10am of weeks 4, 6, 8, 10 and 12

Return Date to Students

One week after the due date

Weighting
15%

Assessment Criteria
In most cases, quiz answers will be automatically marked, with marks awarded based on the correctness of the answer within the context of topics covered in lectures and workshops. Questions may be worth different marks, with the marks indicated in the quiz. If quiz answers are manually marked (e.g. explanation style questions), then marks will be awarded based on the correctness and clarity of the answer.
When multiple attempts are made on a quiz, the highest score of those attempts will count towards your grade. As results and solutions may be released immediately after the due date, late submissions are not accepted. Making no attempts before the due date will result in a score of 0.
You are expected to have reliable Internet access for the duration of each quiz. Loss of a connection or problems with a computer will generally not be accepted as reasons for an extension or additional attempts.

Referencing Style

- Harvard (author-date)

Submission
Online

Learning Outcomes Assessed

- Explain vulnerabilities and attacks, as well as their countermeasures
- Use and compare cryptographic techniques for securing computers and networks
- Design security controls for organisations, such as firewalls, authentication, and access control
- Develop and deploy network security technologies, including encryption software, VPNs and wireless security

Graduate Attributes

- Knowledge
- Communication
- Cognitive, technical and creative skills
- Research
- Self-management
- Ethical and Professional Responsibility

Academic Integrity Statement

As a CQUniversity student you are expected to act honestly in all aspects of your academic work.

Any assessable work undertaken or submitted for review or assessment must be your own work. Assessable work is any type of work you do to meet the assessment requirements in the unit, including draft work submitted for review and feedback and final work to be assessed.

When you use the ideas, words or data of others in your assessment, you must thoroughly and clearly acknowledge the source of this information by using the correct referencing style for your unit. Using others' work without proper acknowledgement may be considered a form of intellectual dishonesty.

Participating honestly, respectfully, responsibly, and fairly in your university study ensures the CQUniversity qualification you earn will be valued as a true indication of your individual academic achievement and will continue to receive the respect and recognition it deserves.

As a student, you are responsible for reading and following CQUniversity's policies, including the **Student Academic Integrity Policy and Procedure**. This policy sets out CQUniversity's expectations of you to act with integrity, examples of academic integrity breaches to avoid, the processes used to address alleged breaches of academic integrity, and potential penalties.

What is a breach of academic integrity?
A breach of academic integrity includes but is not limited to plagiarism, self-plagiarism, collusion, cheating, contract cheating, and academic misconduct. The Student Academic Integrity Policy and Procedure defines what these terms mean and gives examples.

Why is academic integrity important?
A breach of academic integrity may result in one or more penalties, including suspension or even expulsion from the University. It can also have negative implications for student visas and future enrolment at CQUniversity or elsewhere. Students who engage in contract cheating also risk being blackmailed by contract cheating services.

Where can I get assistance?
For academic advice and guidance, the Academic Learning Centre (ALC) can support you in becoming confident in completing assessments with integrity and of high standard.

What can you do to act with integrity?

Be Honest
If your assessment task is done by someone else, it would be dishonest of you to claim it as your own

Seek Help
If you are not sure about how to cite or reference in essays, reports etc, then seek help from your lecturer, the library or the Academic Learning Centre (ALC)

Produce Original Work
Originality comes from your ability to read widely, think critically, and apply your gained knowledge to address a question or problem