



COIT20262 *Advanced Network Security*

Term 2 - 2020

Profile information current as at 24/04/2024 12:28 am

All details in this unit profile for COIT20262 have been officially approved by CQUniversity and represent a learning partnership between the University and you (our student). The information will not be changed unless absolutely necessary and any change will be clearly indicated by an approved correction included in the profile.

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 - 2020

- Brisbane
- Melbourne
- Online
- 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. **Online Quiz(zes)**

Weighting: 25%

2. **Written Assessment**

Weighting: 35%

3. **Written Assessment**

Weighting: 40%

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 evaluations

Feedback

Lab activities should be improved as it was too hard to work on online. Some in-class quizzes must be given more time.

Recommendation

Consider offering brief step-by-step guidance and short video demonstration to complete the tutorial activities and have ample time to complete in-class quizzes.

Feedback from Moodle forum posts by students and staff feedback

Feedback

Virtual network (virtnet) running on VirtualBox sometime gives unexpected error.

Recommendation

Explore the possibility of migration to the cloud environment from VirtualBox

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.

The Australian Computer Society (ACS) recognises the Skills Framework for the Information Age (SFIA). SFIA is adopted by organisations, governments and individuals in many 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.

This unit contributes to the following workplace skills as defined by [SFIA 7](#) (the SFIA code is included):

- Information Security (SCTY)
- Security Administration (SCAD)
- Information Assurance (INAS)
- Specialist Advice (TECH)

Alignment of Learning Outcomes, Assessment and Graduate Attributes



Alignment of Assessment Tasks to Learning Outcomes

Assessment Tasks	Learning Outcomes				
	1	2	3	4	5
1 - Written Assessment - 35%	•	•			•
2 - Online Quiz(zes) - 25%	•	•	•	•	

Textbooks and Resources

Textbooks

COIT20262

Supplementary

Computer Security: Principles and Practice, Global Edition

Edition: 4th (2018)

Authors: William Stallings and Lawrie Brown

Pearson

ISBN: 9781292220635

Binding: eBook

Additional Textbook Information

If you prefer to study with a paper copy, they are available at the CQUni Bookshop here: <http://bookshop.cqu.edu.au> (search on the Unit code). An eBook of "Computer Security: Principles and Practice" is available from the publisher Pearson at <https://www.pearson.com.au/9781292220635>.

[View textbooks at the CQUniversity Bookshop](#)

IT Resources

You will need access to the following IT resources:

- CQUniversity Student Email
- Internet
- Unit Website (Moodle)
- VirtualBox
- WinSCP or FileZilla
- Wireshark
- Zoom
- PuTTY
- Computer with webcam, microphone, speakers and at least 8GB RAM

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 - 13 Jul 2020

Module/Topic	Chapter	Events and Submissions/Topic
Introduction to Network Security	Chapter 1 of <i>Computer Security: Principles and Practice</i> , 4th Edition, 2018 by Stallings and Brown.	

Week 2 - 20 Jul 2020

Module/Topic	Chapter	Events and Submissions/Topic
Network Attacks	Chapter 1	

Week 3 - 27 Jul 2020

Module/Topic	Chapter	Events and Submissions/Topic
Vulnerabilities	Chapter 11 and OWASP Top 10	Quiz 1 (in-class): Due in your allocated tutorial class in Week 3
Week 4 - 03 Aug 2020		
Module/Topic	Chapter	Events and Submissions/Topic
Symmetric Key Cryptography	Chapter 2	
Week 5 - 10 Aug 2020		
Module/Topic	Chapter	Events and Submissions/Topic
Public Key Cryptography	Chapter 2	Quiz 2 (online): Due Week 5 Monday (10 Aug. 2020) 10:00am AEST
Vacation Week - 17 Aug 2020		
Module/Topic	Chapter	Events and Submissions/Topic
Week 6 - 24 Aug 2020		
Module/Topic	Chapter	Events and Submissions/Topic
Firewalls	Chapter 9	Assignment 1 Due: Week 6 Monday (24 Aug 2020) 10:00 am AEST
Week 7 - 31 Aug 2020		
Module/Topic	Chapter	Events and Submissions/Topic
Authentication	Chapter 3	Quiz 3 (in-class): Due in your allocated tutorial class in Week 7
Week 8 - 07 Sep 2020		
Module/Topic	Chapter	Events and Submissions/Topic
Access Control	Chapter 4	
Week 9 - 14 Sep 2020		
Module/Topic	Chapter	Events and Submissions/Topic
Internet Security	Chapter 22	
Week 10 - 21 Sep 2020		
Module/Topic	Chapter	Events and Submissions/Topic
Wireless Security	Chapter 24	Quiz 4 (in-class): Due in your allocated tutorial class in Week 10
Week 11 - 28 Sep 2020		
Module/Topic	Chapter	Events and Submissions/Topic
Virtual Private Networks	Chapter 9	
Week 12 - 05 Oct 2020		
Module/Topic	Chapter	Events and Submissions/Topic
Review and Assignment Completion	-	Quiz 5 (online): Due Week 12 Monday (5 Oct. 2020) 10:00am AEST
Review/Exam Week - 12 Oct 2020		
Module/Topic	Chapter	Events and Submissions/Topic
		Assignment 2 Due: Review/Exam Week Monday (12 Oct 2020) 10:00 am AEST

Term Specific Information

With online delivery this term, you will need access to a computer (laptop or PC) that supports the required software and has video conferencing capabilities. The most important required software is [VirtualBox](#) which will be used to run multiple virtual machines at the same time. Therefore it is highly recommended your computer has at least 8 GB of RAM. If your computer has only 4GB then the software may work, but will likely be slow and inconvenient. In this case you are recommended to contact the Unit Coordinator who can advise how to test whether your computer with 4GB of RAM will be usable in this unit.

Your computer that runs VirtualBox must also have video conferencing capabilities. This includes a webcam, microphone and speakers (or headset). Some tasks may require you to share your screen showing VirtualBox while you are speaking. Therefore you cannot rely on your mobile phone for video conferencing.

Your computer should have virtualisation hardware acceleration, that is, Intel VT-x or AMD-V (depending on your CPU). Most computers have this, but some have it disabled in the BIOS. You will need to search online to find if your computer supports virtualisation hardware acceleration and how to enable it (e.g. search for your laptop model and "enable intel VT-x" or "enable AMD-V"). If your computer does not support this acceleration, then you will need to use an older version of VirtualBox and may find the software slow and inconvenient.

Assessment Tasks

1 Quizzes

Assessment Type

Online Quiz(zes)

Task Description

You will undertake five (5) quizzes on Moodle throughout the term: three (3) of the quizzes must be taken in your assigned tutorial class, while two (2) of the quizzes you may take in your own time (within limits - see below). Each quiz will cover lecture and tutorial topics from the weeks leading up to that quiz. Each quiz will consist of multiple-choice questions, short answer questions, and/or calculations. There will be multiple independent questions in each quiz. All quizzes are individual assessments.

Each quiz will be time-limited, typically allowing you between 15 and 30 minutes to complete the quiz. Quiz time limits, topics, number of attempts allowed and open/close times can be found on Moodle. Read on for more details about in-class and out-of-class quizzes.

In-class quizzes

The three (3) in-class quizzes must be taken in your assigned tutorial class. The quiz will open shortly after the start of your tutorial class and will close after the time limit has been reached. You will be allowed only a single attempt at the in-class quiz, with the score for that attempt counting towards your grade.

In-class quizzes will be held during the tutorials in weeks: 3, 7 and 10. In-class quizzes will be supervised. While they will be open book, you are not allowed to communicate with anyone (including other students or people online) while the quiz is open.

You will not be allowed to take an in-class quiz at any time outside of your assigned tutorial unless an Assessment Extension Request is approved. The quiz will close at the same time for all students in your tutorial. If you arrive late for the tutorial, you will not be granted extra time. Changes to in-class quiz times can only be granted with approval by the Unit Coordinator.

As all tutorial classes are delivered online, all students are required to take the in-class quiz via Zoom screen sharing. All students will need access to a webcam, speakers and microphone (e.g. headset), and be prepared to share their entire screen using Zoom. Zoom must be running on the same computer that the quiz is taken on.

For students studying via distance that do not have a designated class, the Unit Coordinator will negotiate with you a time at which you can undertake a supervised quiz via Zoom screen sharing.

Out-of-class quizzes

The two (2) out-of-class quizzes may be taken between the open and close time. Each quiz will be open for at least one (1) week, that is, it will open at least one week before the due date. You will be allowed multiple attempts (at least 2), with your highest score counting towards your grade.

Out-of-class quizzes will be due Monday at 10 am (AEST) on weeks: 5 and 12. Out-of-class quizzes are unsupervised. While they will be open book, you are expected to complete the quiz on your own, without the assistance of others.

Preparation of your computer and Internet

You are assumed to have a working computer and Internet connection during the term, and especially during times when attempting a quiz. Technical problems, such as a computer crash or loss of Internet connection, will not usually be a reason for an extra attempt or extension. You are expected to prepare your computer before the quiz starts. If problems outside of your control occur during an in-class quiz, report immediately to your tutor, who may either extend

the time or allow you to undertake the quiz at another time (with the Unit Coordinators approval). If problems occur during an out-of-class quiz, you will have the other attempt to rely on. Only in extenuating circumstances will Assessment Extension Requests be granted for quizzes.

Number of Quizzes

5

Frequency of Quizzes

Other

Assessment Due Date

See the task description.

Return Date to Students

One week after the due date

Weighting

25%

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 tutorials. 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 allowed on a quiz, the highest score of those attempts will count towards your grade. As results and solutions may be released shortly after the due date (or in the case of in-class quizzes, after the final tutorial group), late submissions are not accepted. Making no attempts before the due date will result in a score of 0.

Referencing Style

- [Harvard \(author-date\)](#)

Submission

Online

Submission Instructions

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
- Self-management
- Ethical and Professional Responsibility

2 Assignment 1

Assessment Type

Written Assessment

Task Description

This assignment requires you to apply knowledge from the lectures and tutorials 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 apply the knowledge to identify security issues and/or design security mechanisms, study and apply cryptographic tools, as well as research and report on state-of-the-art vulnerabilities, 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. You are assumed to have familiarity with the tools and techniques covered in the tutorials, e.g. VirtualBox and virtnet. You may also be required to submit (parts of) your online journal, which is a record of your activities each week. Details of the online journal can be found on Moodle.

This assignment is an 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 Monday (24 Aug 2020) 10:00 am AEST

Return Date to Students

Week 8 Monday (7 Sept 2020)

Late submissions may be returned to students two weeks after the submission date.

Weighting

35%

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

Submission Instructions

Online through Moodle

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

3 Assignment 2

Assessment Type

Written Assessment

Task Description

This assignment requires you to apply knowledge from the lectures and tutorials 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. You are assumed to have familiarity with the tools and techniques covered in the tutorials, e.g. VirtualBox and virtnet. You may also be required to submit (parts of) your online journal, which is a record of your activities each week. Details of the online journal can be found on Moodle.

This assignment is an 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

Review/Exam Week Monday (12 Oct 2020) 10:00 am AEST

Return Date to Students

This assignment will be returned on Certification of Grades day, as is required of units of no exam

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

Submission Instructions

Online through Moodle

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

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