COIT20262 *Advanced Network Security*
Term 2 - 2023

Profile information current as at 17/04/2024 11:53 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 - 2023

- 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. **Written Assessment**
Weighting: 35%
2. **Online Quiz(zes)**
Weighting: 25%
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 emails

Feedback

Virtual Box was difficult to use on the latest Mac version.

Recommendation

Make it clear that Windows is the only environment supported by the teaching team as the computer labs only have Windows. Explore the possibility of migration to the cloud environment from VirtualBox.

Feedback from Teaching team

Feedback

Update the assessments to improve the complex computing coverage.

Recommendation

Review the assessments and update it with more open-ended and analytical questions.

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)

The National Initiative for Cybersecurity Education (NICE) Framework defines knowledge, skills and tasks needed to perform various cyber security roles. Developed by the National Institute of Standards and Technology (NIST), the NICE Framework is used by organisations to plan their workforce, including recruit into cyber security positions.
This unit helps prepare you for roles such as Systems Security Analyst, Network Operations Specialist and Systems Administrator, contributing to the following knowledge and skills:

- K0005 Knowledge of cyber threats and vulnerabilities.
- K0018 Knowledge of encryption algorithms
- K0019 Knowledge of cryptography and cryptographic key management concepts
- K0044 Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
- K0049 Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).
- K0056 Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).
- K0104 Knowledge of Virtual Private Network (VPN) security.
- K0130 Knowledge of virtualization technologies and virtual machine development and maintenance.
- K0158 Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control).
- K0160 Knowledge of the common attack vectors on the network layer.
- K0179 Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
- K0201 Knowledge of symmetric key rotation techniques and concepts.
- K0339 Knowledge of how to use network analysis tools to identify vulnerabilities.
- K0622 Knowledge of controls related to the use, processing, storage, and transmission of data.
- S0031 Skill in developing and applying security system access controls.
- S0036 Skill in evaluating the adequacy of security designs.
- S0040 Skill in implementing, maintaining, and improving established network security practices.
- S0073 Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).
- S0076 Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware).
- S0077 Skill in securing network communications.
- S0084 Skill in configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection systems).
- S0167 Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).
- S0170 Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate).

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 - 35%	•	•			•
2 - Online Quiz(zes) - 25%	•	•	•	•	
3 - Written Assessment - 40%			•	•	•

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					

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

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
- WEKA (Version: 3.8.1 – 64 Bit)
- 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

MD Mamunur Rashid Unit Coordinator
m.rashid@cqu.edu.au

Schedule

Week 1 - 10 Jul 2023

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

Week 2 - 17 Jul 2023

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

Week 3 - 24 Jul 2023

Module/Topic	Chapter	Events and Submissions/Topic
Vulnerability Analysis and Machine Learning for Network Security	OWASP Top 10	**Quiz 1** (in-class): Due in your allocated tutorial class on Week 3

Week 4 - 31 Jul 2023

Module/Topic	Chapter	Events and Submissions/Topic
Symmetric Key Cryptography	Chapter 2	

Week 5 - 07 Aug 2023

Module/Topic	Chapter	Events and Submissions/Topic
Public Key Cryptography	Chapter 2	**Quiz 2** (online): Due on Week 5 Monday (3 April 2023) 10:00 am AEST

Vacation Week - 14 Aug 2023

Module/Topic	Chapter	Events and Submissions/Topic

Week 6 - 21 Aug 2023

Module/Topic	Chapter	Events and Submissions/Topic
Firewalls	Chapter 9	**Assessment 1** Submission: Due on Week 6 Friday (25 August 2023) 11:45 pm AEST **Assignment 1** Due: Week 6 Friday (25 Aug 2023) 11:45 pm AEST

Week 7 - 28 Aug 2023

Module/Topic	Chapter	Events and Submissions/Topic
Authentication	Chapter 3	**Quiz 3** (in-class): Due in your allocated tutorial class on Week 7

Week 8 - 04 Sep 2023

Module/Topic	Chapter	Events and Submissions/Topic
Access Control	Chapter 4	

Week 9 - 11 Sep 2023

Module/Topic	Chapter	Events and Submissions/Topic
Internet Security	Chapter 22	

Week 10 - 18 Sep 2023

Module/Topic	Chapter	Events and Submissions/Topic
Wireless Security	Chapter 24	**Quiz 4** (in-class): Due in your allocated tutorial class on Week 10

Week 11 - 25 Sep 2023

Module/Topic	Chapter	Events and Submissions/Topic
Virtual Private Networks	Chapter 9	

Week 12 - 02 Oct 2023

Module/Topic	Chapter	Events and Submissions/Topic
Review and Assignment Completion	-	**Quiz 5** (online): Due Week 12 Monday (2 June 2023) 10:00 am AEST

Review/Exam Week - 09 Oct 2023

Module/Topic	Chapter	Events and Submissions/Topic
		Assessment 2 Submission: Due on Review Week Monday (9 October 2023) 11:45 pm AEST **Assignment 2** Due: Review/Exam Week Monday (9 Oct 2023) 11:45 pm AEST

Exam Week - 16 Oct 2023

Module/Topic	Chapter	Events and Submissions/Topic

Assessment Tasks

1 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 Friday (25 Aug 2023) 11:45 pm AEST
Online via Moodle

Return Date to Students
Week 8 Friday (8 Sept 2023)
Online via Moodle

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.

2 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.
For students studying via distance that does 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 times. 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, 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

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 (9 Oct 2023) 11:45 pm AEST
Online via Moodle

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.

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