COIT12202 *Network Security Concepts*
Term 2 - 2018

Profile information current as at 26/04/2024 02:46 pm

General Information

Overview
As the Internet becomes more pervasive, so do the threats to the security of our computer systems and communications. This unit provides you with grounding in security technology. You will study common network security attacks, then the technologies to defend against those attacks. These technologies include cryptography, access control, authentication, firewalls and wireless network protocols. This unit provides security knowledge that is required for industry standard certification exams, such as CompTIA.

Details
Career Level: *Undergraduate*
Unit Level: *Level 2*
Credit Points: *6*
Student Contribution Band: *8*
Fraction of Full-Time Student Load: *0.125*

Pre-requisites or Co-requisites
Prerequisite: COIT12206 OR COIT13147
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
- Cairns
- Distance
- Melbourne
- Rockhampton
- Sydney
- Townsville

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 Undergraduate 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: 15%
2. **Online Quiz(zes)**
Weighting: 10%
3. **Written Assessment**
Weighting: 15%
4. **Online Quiz(zes)**
Weighting: 10%
5. **Examination**
Weighting: 50%

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 Students

Feedback
More hands-on projects should be provided in tutorial lessons.

Recommendation
Design new hands-on workshops for tutorial lessons.

Feedback from Students

Feedback
An open exam or even no exam could be considered for this unit.

Recommendation
A closed book exam is an important part of this unit, as it assesses students' individual knowledge of key concepts. The closed book exam should be maintained, however more flexible methods may be used in the exam. For example, allow students to choose one from multiple provided questions to answer, or provide students with material in the exam that reduces the need for memorisation.

Feedback from Self-reflection

Feedback
Reflect the trend of network security in this unit.

Recommendation
Design some case studies for tutorial lessons and assignments.

Unit Learning Outcomes

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

1. Describe key security concepts and principles
2. Discuss how common security attacks and defences work
3. Explain the role of cryptographic mechanisms in providing computer and network security
4. Apply access control technologies, including firewalls and authentication, to secure computer networks
5. Explain threats and defences that are specific to wireless networks.

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)
- Penetration Testing (PENT)
- Network Support (NTAS)
- Security Administration (SCAD)
- Problem Management (PBMG)
- Data Analysis (DTAN)
- System Design (DESN)
- Incident Management (USUP)

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 - 15%		•	•		
2 - Online Quiz(zes) - 10%	•				
3 - Written Assessment - 15%				•	•
4 - Online Quiz(zes) - 10%	•				
5 - Examination - 50%		•	•	•	•

Alignment of Graduate Attributes to Learning Outcomes

Graduate Attributes	Learning Outcomes				
	1	2	3	4	5
1 - Communication	•	•	•		•
2 - Problem Solving	•	•	•	•	•
3 - Critical Thinking				•	•
4 - Information Literacy			•		•
5 - Team Work					
6 - Information Technology Competence		•		•	
7 - Cross Cultural Competence					
8 - Ethical practice		•			
9 - Social Innovation					
10 - 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	9	10
1 - Written Assessment - 15%	•	•		•		•		•		
2 - Online Quiz(zes) - 10%	•	•								

Assessment Tasks	Graduate Attributes									
	1	2	3	4	5	6	7	8	9	10
3 - Written Assessment - 15%	•	•	•	•		•				
4 - Online Quiz(zes) - 10%	•	•								
5 - Examination - 50%	•	•	•	•		•		•		

Textbooks and Resources

Textbooks

COIT12202

Prescribed

CompTIA security+ guide to network security fundamentals
Edition: 5th (2015)
Authors: Ciampa, M
Cengage
Boston , Massachusetts , USA
ISBN: 978-1-305-09394-2 / 978-1-305-09391-1
Binding: Hardcover

View textbooks at the CQUniversity Bookshop

IT Resources

You will need access to the following IT resources:

- CQUniversity Student Email
- Internet
- Unit Website (Moodle)
- HashTab - a GUI hash Generator
- KeePass - A Free Open Source Password Manager
- keylogger - A Type of Surveillance Software
- SMAC 2.0 - MAC Address Changer
- Snort - Network Intrusion Prevention And Detection System (NIPS - NIDS)
- VirtualBox - A Virtualization Software Package
- Wireshark - Network Protocol Analyser

Referencing Style

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

Teaching Contacts

Yufeng Lin Unit Coordinator
y.lin@cqu.edu.au

Schedule

Week 1 - 09 Jul 2018

Module/Topic	Chapter	Events and Submissions/Topic

Introduction to Security	Introduction to Security (Ciampa, M. Chapter 1)	

Week 2 - 16 Jul 2018

Module/Topic	Chapter	Events and Submissions/Topic
Threats	Malware (Ciampa, M. Chapter 2); and Application and Network Attacks (Ciampa, M. Chapter 3)	

Week 3 - 23 Jul 2018

Module/Topic	Chapter	Events and Submissions/Topic
Cryptography: Basic	Basic Cryptography (Ciampa, M. Chapter 5)	

Week 4 - 30 Jul 2018

Module/Topic	Chapter	Events and Submissions/Topic
Cryptography: Advanced	Advanced Cryptography (Ciampa, M. Chapter 6)	

Week 5 - 06 Aug 2018

Module/Topic	Chapter	Events and Submissions/Topic
Key Management and Distribution	Online resources and other reference books (needed learning materials will be provided): • PKI (Ciampa, M. Security+ Guide to Network Security Fundations, Sixth Edition, Chapter 4) • Key Management and Distribution (Stallings, W. Cryptography and Network Security: Principles and Practice, Seventh Edition, Chapter 14)	

Vacation Week - 13 Aug 2018

Module/Topic	Chapter	Events and Submissions/Topic

Week 6 - 20 Aug 2018

Module/Topic	Chapter	Events and Submissions/Topic
Network Security I	Network Security (Ciampa, M. Chapter 7)	**SHORT-ANSWER QUESTIONS - 1** Due: Week 6 Monday (20 Aug 2018) 11:45 pm AEST **Online Quiz - 1** Due: Week 6 Friday (24 Aug 2018) 11:45 pm AEST

Week 7 - 27 Aug 2018

Module/Topic	Chapter	Events and Submissions/Topic
Network Security II	Administering a Secure Network (Ciampa, M. Chapter 8)	

Week 8 - 03 Sep 2018

Module/Topic	Chapter	Events and Submissions/Topic
Access Control	Access Control Fundamentals (Ciampa, M. Chapter 11)	

Week 9 - 10 Sep 2018

Module/Topic	Chapter	Events and Submissions/Topic
Identity Management	Authentication and Account Management (Ciampa, M. Chapter 12);	

Week 10 - 17 Sep 2018

Module/Topic	Chapter	Events and Submissions/Topic

Mobile Security I	Wireless Network Security (Ciampa, M. Chapter 9)	

Week 11 - 24 Sep 2018

Module/Topic	Chapter	Events and Submissions/Topic
Mobile Security II	Mobile Device Security (Ciampa, M. Chapter 10)	**SHORT-ANSWER QUESTIONS - 2** Due: Week 11 Friday (28 Sept 2018) 11:45 pm AEST

Week 12 - 01 Oct 2018

Module/Topic	Chapter	Events and Submissions/Topic
Compliance and Operational Security	Business Continuity (Ciampa, M. Chapter 13); and Risk Mitigation (Ciampa, M. Chapter 14)	**Online Quiz - 2** Due: Week 12 Friday (5 Oct 2018) 11:45 pm AEST

Review/Exam Week - 08 Oct 2018

Module/Topic	Chapter	Events and Submissions/Topic

Exam Week - 15 Oct 2018

Module/Topic	Chapter	Events and Submissions/Topic

Assessment Tasks

1 SHORT-ANSWER QUESTIONS - 1

Assessment Type
Written Assessment

Task Description
SHORT-ANSWER QUESTIONS - 1 is designed to test your understanding of information security including the basic concepts of information security, threats, cryptography and key management and distribution. The assessment task contains a series of short-answer questions relating to the contents covered in weeks 1-5. Further details, including what you are required to submit, will be available on the Moodle website.

Assessment Due Date
Week 6 Monday (20 Aug 2018) 11:45 pm AEST

Return Date to Students
Week 8 Monday (3 Sept 2018)
Assessments will be returned through Moodle. Late submissions with or without extension approvals may be returned after the above date.

Weighting
15%

Assessment Criteria
For short-answer questions, the answers will be assessed in regards to accuracy, clarity and detail. A template with detailed tabular marking criteria will be provided on Moodle. Assignments received 14 days or more after the due date will not be marked and will receive zero.

Referencing Style

- Harvard (author-date)

Submission
Online

Submission Instructions
Submission instructions are provided in Moodle.

Learning Outcomes Assessed

- Discuss how common security attacks and defences work
- Explain the role of cryptographic mechanisms in providing computer and network security

Graduate Attributes

- Communication
- Problem Solving
- Information Literacy
- Information Technology Competence
- Ethical practice

2 Online Quiz - 1

Assessment Type
Online Quiz(zes)

Task Description
The quiz consists of a series of 30 True/False and Multiple Choice questions. Questions will be randomly selected from a pool of questions on topics in weeks 1 to 5. You are unlikely to be asked the same questions as other other students, nor the same questions in subsequent attempts at the quiz. The time limit for each attempt is 45 minutes. The quiz automatically closes - if you have not submitted an attempt at the quiz by the due date, you will receive zero. Quizzes that are open (or being attempted) at the time the quiz closes will not (and cannot) be submitted.
You are allowed to attempt the quiz as many times as you want, however, the result of your last submission will be your final mark of the quiz.

Number of Quizzes

Frequency of Quizzes

Assessment Due Date
Week 6 Friday (24 Aug 2018) 11:45 pm AEST

Return Date to Students
Week 6 Friday (24 Aug 2018)
Immediately after the quiz closes.

Weighting
10%

Assessment Criteria
The quiz is automatically graded by the system based on the selection of correct or incorrect answers. Each attempt will be marked after you submit your answers. The result of your last submission will be your final mark of the quiz. Extensions are not possible for quizzes. If you miss the quiz, you cannot do it later.

Referencing Style

- Harvard (author-date)

Submission
Online

Learning Outcomes Assessed

- Describe key security concepts and principles

Graduate Attributes

- Communication
- Problem Solving

3 SHORT-ANSWER QUESTIONS - 2

Assessment Type
Written Assessment

Task Description
SHORT-ANSWER QUESTIONS - 2 is designed to test your understanding of network security, including wireless network security, mobile security, access control and identity management. The assessment task contains a series of short-answer questions relating to the contents covered in weeks 6-10. Further details, including what you are required to submit, will be available on the Moodle website.

Assessment Due Date
Week 11 Friday (28 Sept 2018) 11:45 pm AEST

Return Date to Students
Review/Exam Week Friday (12 Oct 2018)
Assessments will be returned through Moodle. Late submissions with or without extension approvals may be returned after the above date.

Weighting
15%

Assessment Criteria
For short-answer questions, the answers will be assessed in regards to accuracy, clarity and detail. A template with detailed tabular marking criteria will be provided on Moodle. Assignments received 14 days or more after the due date will not be marked and will receive zero.

Referencing Style

- Harvard (author-date)

Submission
Online

Submission Instructions
Submission instructions are provided in Moodle.

Learning Outcomes Assessed

- Apply access control technologies, including firewalls and authentication, to secure computer networks
- Explain threats and defences that are specific to wireless networks.

Graduate Attributes

- Communication
- Problem Solving
- Critical Thinking
- Information Literacy
- Information Technology Competence

4 Online Quiz - 2

Assessment Type
Online Quiz(zes)

Task Description
The quiz consists of a series of 30 True/False and Multiple Choice questions. Questions will be randomly selected from a pool of questions on topics in weeks 6 to 11. You are unlikely to be asked the same questions as other other students, nor the same questions in subsequent attempts at the quiz. The time limit for each attempt is 45 minutes. The quiz automatically closes - if you have not submitted an attempt at the quiz by the due date, you will receive zero. Quizzes that are open (or being attempted) at the time the quiz closes will not (and cannot) be submitted.
You are allowed to attempt the quiz as many times as you want, however, the result of your last submission will be your final mark of the quiz.

Number of Quizzes

Frequency of Quizzes

Assessment Due Date
Week 12 Friday (5 Oct 2018) 11:45 pm AEST

Return Date to Students
Week 12 Friday (5 Oct 2018)
Immediately after the quiz closes.

Weighting
10%

Assessment Criteria
The quiz is automatically graded by the system based on the selection of correct or incorrect answers. Each attempt will be marked after you submit your answers. The result of your last submission will be your final mark of the quiz. Extensions are not possible for quizzes. If you miss the quiz, you cannot do it later.

Referencing Style

- Harvard (author-date)

Submission
Online

Learning Outcomes Assessed

- Describe key security concepts and principles

Graduate Attributes

- Communication
- Problem Solving

Examination

Outline
Complete an invigilated examination.

Date
During the examination period at a CQUniversity examination centre.

Weighting
50%

Length
120 minutes

Exam Conditions
Closed Book.

Materials
Dictionary - non-electronic, concise, direct translation only (dictionary must not contain any notes or comments).

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