COIT12202 *Network Security Concepts*
Term 2 - 2017

Profile information current as at 14/12/2025 04:55 am

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 students with grounding in security technology. Topics include network security fundamentals, access control and authentication, firewalls, wireless network security, intrusion detection systems and cryptographic techniques and their applications. The unit provides the knowledge requirements to sit the CompTIA Security and industry standard certification exam should students choose to once they have gained the required industry experience.

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 - 2017

- 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: 25%
2. **Written Assessment**
Weighting: 25%
3. **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 Student Feedback

Feedback
More supporting software need to be installed in lab computers to perform tutorial.

Recommendation
Effective communication will be conducted with TaSAC to seek more support with needed software installation.

Feedback from Student Feedback

Feedback
An open book exam

Recommendation
More flexible examination methods will be provided.

Feedback from Self-reflection

Feedback
Lab activities

Recommendation
Hands-on projects will be designed based on different operating systems to enhance understanding on the knowledge of network security.

Unit Learning Outcomes

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

1. Discuss general security concepts and define basic terminology
2. Explain the role of network security technologies such as firewalls, intrusion detection systems and authentication
3. Assess wireless security infrastructure and recognise threats and weaknesses
4. Explain cryptographic mechanisms used to provide security
5. Describe methods and technologies used to achieve operational and organisational security
6. Apply the knowledge gained in the unit in practical exercises using common hardware and software

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:

- Network Support (NTAS)
- Problem Management (PBMG)
- Data Analysis (DTAN)
- System Design (DESN)
- Service Desk and 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	6
1 - Written Assessment - 25%	•	•		•		•
2 - Written Assessment - 25%	•	•	•			•
3 - Examination - 50%	•	•	•	•	•	•

Alignment of Graduate Attributes to Learning Outcomes

Graduate Attributes	Learning Outcomes					
	1	2	3	4	5	6
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 - 25%	•	•	•			•		•		
2 - Written Assessment - 25%	•	•	•			•		•		
3 - Examination - 50%	•	•	•			•	•	•		

Textbooks and Resources

Textbooks

COIT12202

Prescribed

CompTIA security+ guide to network security fundamentals
Edition: 5th (2015)
Authors: Ciampa, M
Cengage
Boston , 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)
- Bluestacks Android Emulator - An Android OS Emulator
- 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 - 10 Jul 2017

Module/Topic	Chapter	Events and Submissions/Topic
Introduction to Security	Introduction to Security (Ciampa, M. Chapter 1)	

Week 2 - 17 Jul 2017

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

Week 3 - 24 Jul 2017

Module/Topic	Chapter	Events and Submissions/Topic

Application, Data, and Host Security	Host, Application, and Data Security (Ciampa, M. Chapter 4)	

Week 4 - 31 Jul 2017

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

Week 5 - 07 Aug 2017

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

Vacation Week - 14 Aug 2017

Module/Topic	Chapter	Events and Submissions/Topic

Week 6 - 21 Aug 2017

Module/Topic	Chapter	Events and Submissions/Topic
Network Security I	Network Security (Ciampa, M. Chapter 7)	**Quiz + Short-Answer Questions - 1** Due: Week 6 Friday (25 Aug 2017) 11:45 pm AEST

Week 7 - 28 Aug 2017

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

Week 8 - 04 Sep 2017

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

Week 9 - 11 Sep 2017

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

Week 10 - 18 Sep 2017

Module/Topic	Chapter	Events and Submissions/Topic
Mobile Security I	Wireless Network Security (Ciampa, M. Chapter 9)	**Quiz + Short-Answer Questions - 2** Due: Week 10 Friday (22 Sept 2017) 11:45 pm AEST

Week 11 - 25 Sep 2017

Module/Topic	Chapter	Events and Submissions/Topic
Mobile Security II	Mobile Device Security (Ciampa, M. Chapter 10)	

Week 12 - 02 Oct 2017

Module/Topic	Chapter	Events and Submissions/Topic
Compliance and Operational Security	Business Continuity (Ciampa, M. Chapter 13); and Risk Mitigation (Ciampa, M. Chapter 14)	

Review/Exam Week - 09 Oct 2017

Module/Topic	Chapter	Events and Submissions/Topic

Exam Week - 16 Oct 2017

Module/Topic	Chapter	Events and Submissions/Topic

Assessment Tasks

1 Quiz + Short-Answer Questions - 1

Assessment Type
Written Assessment

Task Description
Assignment 1 is designed to test your understanding of information security including the background of information security, threats, application, data and host security, basic and advanced cryptography. This task contains two parts, quiz questions (10%) and a series of short-answer questions (15%) relating to the contents in weeks 1-5. Further details and what you are required to submit will be available on the Moodle website in Week 2.

Assessment Due Date
Week 6 Friday (25 Aug 2017) 11:45 pm AEST

Friday 25-Aug-2017 11:45 PM AEST (Australian Eastern Standard Time)

Return Date to Students
Week 8 Friday (8 Sept 2017)

Friday 08-Sep-2017

Weighting
25%

Assessment Criteria
The quiz is automatically graded by the system based on the selection of correct or incorrect answers. For short-answer questions, a template with a detailed tabular marking criteria will be provided and the answers will be assessed in regards to accuracy, clarity and detail.

Referencing Style

- Harvard (author-date)

Submission
Online

Submission Instructions
Submission instructions are provided in Moodle.

Learning Outcomes Assessed

- Discuss general security concepts and define basic terminology
- Explain the role of network security technologies such as firewalls, intrusion detection systems and authentication
- Explain cryptographic mechanisms used to provide security
- Apply the knowledge gained in the unit in practical exercises using common hardware and software

Graduate Attributes

- Communication
- Problem Solving
- Critical Thinking
- Information Technology Competence
- Ethical practice

2 Quiz + Short-Answer Questions - 2

Assessment Type
Written Assessment

Task Description
Assignment 2 is designed to test your understanding of network security, including network security, mobile security, access control and Identity Management. This task contains two parts, quiz questions (10%) and a series of short-answer questions (15%) relating to the contents in weeks 6-10. Further details and what you are required to submit will be available on the Moodle website.

Assessment Due Date
Week 10 Friday (22 Sept 2017) 11:45 pm AEST

Friday 22-Sep-2017 11:45 PM AEST (Australian Eastern Standard Time)

Return Date to Students
Week 12 Friday (6 Oct 2017)

Friday 13-Oct-2017

Weighting
25%

Assessment Criteria
The quiz is automatically graded. Short-answer questions will be assessed against the criteria of accuracy, clarity and detail.

Referencing Style

- Harvard (author-date)

Submission
Online

Submission Instructions
Submission instructions are provided in Moodle.

Learning Outcomes Assessed

- Discuss general security concepts and define basic terminology
- Explain the role of network security technologies such as firewalls, intrusion detection systems and authentication
- Assess wireless security infrastructure and recognise threats and weaknesses
- Apply the knowledge gained in the unit in practical exercises using common hardware and software

Graduate Attributes

- Communication
- Problem Solving
- Critical Thinking
- Information Technology Competence
- Ethical practice

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
Calculator - non-programmable, no text retrieval, silent only
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