# COIT20262 *Advanced Network Security*
## Term 2 - 2017

Profile information current as at 06/05/2024 05:15 am



## General Information

### Overview
This unit provides student with a complete understanding of how to protect the integrity, confidentiality, and availability of information and network services in business organisations. Students will study advanced topics in security technology including 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 examination should students choose to once they have gained the required industry experience. Note: If students have undertaken COIS23001 Network Security then this unit cannot be taken.

### 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 - 2017

- 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. **Practical and Written Assessment**
Weighting: 40%
2. **Group Discussion**
Weighting: 10%
3. **Practical and Written Assessment**
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, Teaching team

**Feedback**
More detailed instructions in workshop tasks

**Recommendation**
Include detailed examples and/or videos for each workshop activity.

#### Feedback from Teaching team

**Feedback**
Some lectures are too long, cover irrelevant content

**Recommendation**
Revise lecture material, identifying content to be updated and improved.

## Unit Learning Outcomes

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

1. Plan organisational adoption of security controls such as proxies, firewalls and intrusion detection systems.
2. Design secure wired and wireless network infrastructure with encryption and enterprise level authentication.
3. Synthesise the knowledge gained in the unit to address organisational security using policies and procedures, hardware and software.
4. Formulate security countermeasures to reduce potential security risks.
5. Analyse emerging security threats and 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 |

| Assessment Tasks | Learning Outcomes | | | | |
|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |
| 1 - Practical and Written Assessment - 40% | • | • | • | • | • |
| 2 - Group Discussion - 10% | • | • | • | • | • |
| 3 - Practical and Written Assessment - 50% | • | • | • | • | • |

## 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 - Practical and Written Assessment - 40% | ◦ | | ◦ | ◦ | | ◦ | | |
| 2 - Group Discussion - 10% | ◦ | ◦ | ◦ | ◦ | ◦ | ◦ | | |
| 3 - Practical and Written Assessment - 50% | ◦ | | ◦ | ◦ | | ◦ | | |

## Textbooks and Resources

### Textbooks

COIT20262

**Prescribed**

**Guide to Firewall & VPNs**
Edition: 3rd (Note: Chapters 4, 5, 6, 7, and 10 only) (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 (Note: Chapters 3 and 8 only) (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.

**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

## 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 - 10 Jul 2017**

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

**Week 2 - 17 Jul 2017**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| Attacks: Malware, Social Engineering, Application and Network-based Attacks | Ciampa: Chapters 2 & 3 | |

**Week 3 - 24 Jul 2017**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| Vulnerability Assessment; and Host, Application, and Data Security | Ciampa: Chapters 15 & 4 | |

**Week 4 - 31 Jul 2017**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| Cryptography | Ciampa: Chapter 5 | Peerwise Learning Activity Q1 due 9am Monday |

**Week 5 - 07 Aug 2017**

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

**Vacation Week - 14 Aug 2017**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|

**Week 6 - 21 Aug 2017**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| Firewall Configuration and Proxy Servers | Whitman: Chapters 6 & 7 | Peerwise Learning Activity Q2 due 9am Monday<br><br>**Assignment 1** Due: Week 6 Friday (25 Aug 2017) 5:00 pm AEST |

**Week 7 - 28 Aug 2017**

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

**Week 8 - 04 Sep 2017**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| Access Control | Ciampa: Chapter 11 | Peerwise Learning Activity Q3 due 9am Monday |

**Week 9 - 11 Sep 2017**

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

**Week 10 - 18 Sep 2017**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| Virtual Private Networks | Weaver: Chapter 11; Whitman: Chapter 10 | Peerwise Learning Activity Q4 due 9am Monday |

**Week 11 - 25 Sep 2017**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|

| | | |
|---|---|---|
| Wireless Network Security | Ciampa: Chapter 9 | |

**Week 12 - 02 Oct 2017**

| Module/Topic | Chapter | Events and Submissions/Topic |
|---|---|---|
| Intrusion Detection and Prevention Systems | Weaver: Chapter 8 | Peerwise Learning Activity Q5 due 9am Monday<br><br>**Assignment 2** Due: Week 12 Friday (6 Oct 2017) 5:00 pm AEST |

**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 Assignment 1

**Assessment Type**
Practical and Written Assessment

**Task Description**
This assignment requires you to apply knowledge from the lectures 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; design and configure firewalls as a means of network access control; 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. The report may be a mix of short answers, diagrams, tables, and short essays with references. Questions, and expected structure/format of the report, can be found on Moodle.

**Assessment Due Date**
Week 6 Friday (25 Aug 2017) 5:00 pm AEST

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

**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. Mark allocation for each question, the expected format of the answer, and details of the marking criteria can be found in the assignment on Moodle.

**Referencing Style**

- Harvard (author-date)

**Submission**
Online

**Learning Outcomes Assessed**

- Plan organisational adoption of security controls such as proxies, firewalls and intrusion detection systems.
- Design secure wired and wireless network infrastructure with encryption and enterprise level authentication.
- Synthesise the knowledge gained in the unit to address organisational security using policies and procedures, hardware and software.
- Formulate security countermeasures to reduce potential security risks.

- Analyse emerging security threats and controls.

**Graduate Attributes**

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

## 2 PeerWise Learning Activity (PLA)

**Assessment Type**
Group Discussion

**Task Description**
This term you will be using a peer-directed learning activity called Peerwise. The goal is that you equally engage and participate in both spontaneous and formally structured student-student learning interactions. There will be five tasks during the term. In each task you must create a multiple choice question on the allocated topic, and must answer questions created by other students. Please refer to the Moodle site for a complete description of the task, including the number of questions to be answered.

**Assessment Due Date**

9am Monday morning in weeks 4, 6, 8, 10 and 12

**Return Date to Students**

On certification day

**Weighting**
10%

**Assessment Criteria**
For each of the five tasks, the creation of your own multiple choice question is worth 50% and the answering of other students multiple choice questions is worth 50%. For creating the question you will be assessed on the novelty, appropriateness and clarity of the question, the set of possible answers and the explanation of the correct answer. For answering other students questions you will be assessed on the number of questions answered and your feedback given on those answered questions. Peer assessment as well as instructor assessment will be used.
All submissions after the deadline will receive 0 marks. Late submissions will not be accepted. Submissions copied from other sources (e.g. websites, textbook) are not allowed; the questions should be novel, i.e. new and original.

**Referencing Style**

- Harvard (author-date)

**Submission**
Online

**Learning Outcomes Assessed**

- Plan organisational adoption of security controls such as proxies, firewalls and intrusion detection systems.
- Design secure wired and wireless network infrastructure with encryption and enterprise level authentication.
- Synthesise the knowledge gained in the unit to address organisational security using policies and procedures, hardware and software.
- Formulate security countermeasures to reduce potential security risks.
- Analyse emerging security threats and controls.

**Graduate Attributes**

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

## 3 Assignment 2

**Assessment Type**
Practical and Written Assessment

**Task Description**
This assignment requires you to apply knowledge from the lectures to solve practical problems, focussing especially on current network security technologies. You will: use software to identify security attacks in network communications; use software to apply encryption techniques to provide confidentiality and authentication; 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. The report may be a mix of short answers, diagrams, tables, and short essays with references. Questions, and expected structure/format of the report, can be found on Moodle.

**Assessment Due Date**
Week 12 Friday (6 Oct 2017) 5:00 pm AEST

**Return Date to Students**

On certification day

**Weighting**
50%

**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. Mark allocation for each question, the expected format of the answer, and details of the marking criteria can be found in the assignment on Moodle.

**Referencing Style**

- Harvard (author-date)

**Submission**
Online

**Learning Outcomes Assessed**

- Plan organisational adoption of security controls such as proxies, firewalls and intrusion detection systems.
- Design secure wired and wireless network infrastructure with encryption and enterprise level authentication.
- Synthesise the knowledge gained in the unit to address organisational security using policies and procedures, hardware and software.
- Formulate security countermeasures to reduce potential security risks.
- Analyse emerging security threats and controls.

**Graduate Attributes**

- Knowledge
- Cognitive, technical and creative skills
- Research
- 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