In Progress

Please note that this Unit Profile is still in progress. The content below is subject to change.

COIT20262 *Advanced Network Security*

Term 2 - 2024

Profile information current as at 19/05/2024 11:16 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 - 2024

- 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

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

Information for Textbooks and Resources has not been released yet.

This information will be available on Monday 17 June 2024

Academic Integrity Statement

Information for Academic Integrity Statement has not been released yet.

This unit profile has not yet been finalised.