Course Outline

Security Principles

INFS 5115 Study Period 5 - 2021

Internal - Mawson Lakes Campus

University of South Australia

Introduction

Welcome

Welcome to INFS 5115 Security Principles. This course aims to assist students in developing a balanced organisational and technical perspective of the principle elements of cybersecurity. Security professionals make use of a wide range of advanced technical skills and expertise. In order to gain maximum value from these skills and expertise, professionals must be able to understand and articulate security issues within a business context from a management perspective. Security issues can be considered from various perspectives, including people, processes and technology, and contemporary security professionals need to consolidate these views and provide a balanced security perspective.

In this course, students will gain advanced skills and knowledge in the following:

- Core security principles including confidentiality, integrity and availability (CIA).
- The contemporary cybersecurity threat landscape.
- End-to-end security implementation for a corporate network.
- Principles of symmetric and asymmetric cryptography.
- Roles and responsibilities of a cybersecurity professional.

I hope that you will find this course interesting and engaging, and that it provides valuable additions to your professional knowledge.

Mr Stephen Hindle
Course Coordinator

Academic Work Definitions

Internal mode includes face to face/in person components such as lectures, tutorials, practicals, workshops or seminars that may be offered at a University campus or delivered at another location. Courses delivered in internal mode may also be offered intensively allowing them to be completed in a shorter period of time. There is an expectation that students will be physically present for the delivery of face to face/in person teaching and learning activities.

Seminar

Student information

A seminar is facilitated learning either in person, or online in a virtual classroom environment, in which you and other students in the course are expected to develop, and be prepared to demonstrate an understanding of specific assigned material in the course via guided discussion by an expert academic or guest speaker. You may also be asked to discuss assigned material in the context of a broader framework of knowledge.

All students are expected to be familiar with relevant assigned source material prior to participation, and to actively engage in group discussions, activities and/or presentation.

Course Teaching Staff

Course Coordinator:	Mr Stephen Hindle
Location:	UniSA STEM
Email:	Stephen.Hindle@unisa.edu.au
Staff Home Page:	people.unisa.edu.au/Stephen.Hindle

* Please refer to your Course homepage for the most up to date list of course teaching staff.

Contact Details

UniSA STEM

Website:	https://www.unisa.edu.au/about-unisa/academic-units/stem/

Additional Contact Details

Instructor: Mr Stephen Hindle

Email : stephen.hindle@unisa.edu.au

Stfaff Home page : https://people.unisa.edu.au/Stephen.Hindle

Course Overview

Prerequisite(s)

Students in LBCP or LHSG must have completed 36 units prior to enrolling in this course.

Corequisite(s)

There are no corequisite courses to be completed in conjunction with this course.

Course Aim

To develop a balanced organisational and technical perspective of the principal elements of cybersecurity.

Course Objectives

On completion of this course, students should be able to:

CO1. Examine and explain a range contemporary cybersecurity threats from a technical perspective.

CO2. Evaluate and communicate the potential impact of cybersecurity threats within an organisational context.

CO3. Apply ethical considerations to the role of a cybersecurity professional in a variety of contexts.

CO4. Research and apply established theories to the discipline of cybersecurity and its professional practice.

Upon completion of this course, students will have achieved the following combination of Graduate Qualities and Course Objectives:

	Graduate Qualities being assessed through the course						
	GQ1	GQ2	GQ3	GQ4	GQ5	GQ6	GQ7
CO1	•	•	•				•
CO2	•		•				
CO3	•				•	•	
CO4		•		•			

Graduate Qualities

A graduate of UniSA:

GQ1. operates effectively with and upon a body of knowledge of sufficient depth to begin professional practice

GQ2. is prepared for life-long learning in pursuit of personal development and excellence in professional practice

GQ3. is an effective problem solver, capable of applying logical, critical, and creative thinking to a range of problems

GQ4. can work both autonomously and collaboratively as a professional

GQ5. is committed to ethical action and social responsibility as a professional and citizen

GQ6. communicates effectively in professional practice and as a member of the community

GQ7. demonstrates international perspectives as a professional and as a citizen

Course Content

In this course, students will gain advanced skills and knowledge in the following:

- Core security principles including confidentiality, integrity and availability (CIA).
- The contemporary cybersecurity threat landscape.
- End-to-end security implementation for a corporate network.
- Principles of symmetric and asymmetric cryptography.
- Roles and responsibilities of a cybersecurity professional.

Teaching and Learning Arrangements

Seminar	2 hours x 13 weeks

Unit Value

4.5 units

Use of recorded material

This course will involve the production of audio and/or video recordings of UniSA students. To protect student privacy, you must not at any time disclose, reproduce or publish these recordings, or related material, in the public domain including online, unless the videoed students give consent for reproduction, disclosure or publication. This requirement is consistent with University statutes, by-laws, policies, rules and guidelines which you agreed to abide by when you signed the Student Enrolment Declaration.

Learning Resources

Textbook(s)

There are no textbooks listed for this course.

Materials to be accessed online

learnonline course site

All course related materials can be accessed through your learn**online** course site which you will be able to access from the my Courses section in myUniSA.

myUniSA

All study related materials can be accessed through: https://my.unisa.edu.au

Assessment

Assessment Details

Details of assessment submission and return are listed under each assessment task. Assessment tasks will be returned to you within two to three weeks of submission.

Cover sheets

A cover sheet is not required for assessment tasks submitted via learnonline, as the system automatically generates one.

If the Course Coordinator allows submissions in hard copy format, you will be required to attach an Assignment Cover Sheet which is available on the learnonline student help (https://lo.unisa.edu.au/mod/book/view.php?id=1843&chapterid=567) and in myUniSA.

Assessment Summary

#	Form of assessment	Length	Duration	Weighting	Due date (Adelaide Time)	Submit via	Objectives being assessed
1	Continuous assessment	N/A	Fortnightly	40%	*See assessment activities for details*	*See assessment activities for details*	CO1, CO2, CO3
2	Presentation	N/A	10 minutes	30%	8 Oct 2021, 11:59 PM	learnonline	CO1, CO2, CO3, CO4
3	Test	N/A	2 hours	30%	See assessment activities for details	In person	CO1, CO2, CO3

Feedback proformas

The feedback proforma is available on your course site.

Assessments

Continuous assessment (Graded)

Assessment Activities

Name	Sub-weighting	Due date (Adelaide Time)	Submit via
Continuous Assessment 1	25%	13 Aug 2021, 11:59 PM	learnonline
Week 2 Weekly Assessment Cryptography	6.25%	6 Aug 2021, 11:59 PM	learnonline
Week 4 Weekly Assessment Cyber Intrusions	6.25%	20 Aug 2021, 11:59 PM	learnonline
Continuous Assessment 2	25%	3 Sep 2021, 11:59 PM	learnonline
Week 6 Weekly Assessment Social Engineering	6.25%	3 Sep 2021, 11:59 PM	learnonline
Week 9 Weekly Assessment Insider Attacks	6.25%	8 Oct 2021, 11:59 PM	learnonline
Continuous Assessment 3	25%	15 Oct 2021, 11:59 PM	learnonline

This assessments consists of multiple activities. Further detail will be provided on the course website.

Presentation (Graded)

Current Cybersecurity Trends: A recorded PowerPoint presentation based on research into a current trend in cybersecurity.

Select and research one of the following topics and prepare a short (10 minute) presentation:

- ***Security Issues with 'Shadow IT' and BYOD:***
  The organisational IT landscape and culture are shifting with less centralised control and an increase in the diversity of services and devices. Managing the security issues associated with this new environment is a substantial challenge for practitioners. What are the major tools and techniques, both technical and managerial, that organisations can leverage to address the inherent risks while still facilitating adequate flexibility?

- ***Encrypted Communications:***
  The issue of encrypted communications has received extensive media coverage in recent times. There are a wide variety of differing perspectives on the topic of who should hold encryption keys and/or the means to retrieve plaintext communications content (e.g. governments vs corporations vs users). What are the differing perspectives on this topic and how can they be reconciled?

- ***Machine Learning In Cybersecurity:***
  Machine learning has become critical to cybersecurity. Machine Learning relies on data from various sources to produce patterns that can be manipulated by algorithms.
  What are some of the sources of this data and how is Machine Learning helping in the fight against Cybersecurity incidents? Choose an area of Cybersecurity and apply the questions posed above.

- ***Zero Trust:***
  The Zero Trust Network model was created in 2010 by John Kindervag, who at the time was a principal analyst at Forrester Research Inc. Zero Trust is a security concept centered on the belief that organizations should not automatically trust anything inside or outside its perimeters and instead must verify anything and everything trying to connect to its systems before granting access. Choose an area of industry then research and design a zero trust model for that Industry.

  You should prepare and submit a 10-minute narrated PowerPoint presentation (i.e. a PowerPoint presentation with embedded audio recording). You also need to prepare a script for this presentation and submit the script as a pdf document. In summary, this submission requires two separate files - a PowerPoint presentation with embedded audio and a pdf document that includes a verbatim script of the narration.

  A minimum of five references from scholarly books, academic journals or conference proceedings is required for this assessment, however substantially more references are recommended.

  Further detail regarding this assessment, including the feedback form, will be published on the course website.

Final Test (Graded)

All of the content in this course is examinable. The final test will be set during the exam period for SP5.

Submission and return of assessment tasks

Most assessments will be uploaded to LearnOnline unless another method is explicitly discussed.

Exam Arrangements

Students will receive advance notice of scheduled examination. All students are required to sit their examination at the scheduled date, time and location irrespective of any conflict with a planned holiday or special event. Internal students are required to sit their examination on-campus or at the central exam venue as stated on the examination timetable.
More information about examination procedures and arrangements for students can be found by consulting the relevant policy http://i.unisa.edu.au/policies-and-procedures/codes/assessment-policies/ (Section 6)

Supplementary Assessment

Supplementary assessment or examination offers students an opportunity to gain a supplementary pass (SP) and is available to all students under specific conditions unless supplementary assessment or examination has not been approved for the course.

Specific conditions and further information is available in section 7 of the Assessment Policy and Procedures Manual.
http://i.unisa.edu.au/policies-and-procedures/codes/assessment-policies/

Important information about all assessment

All students must adhere to the University of South Australia's policies about assessment:
http://i.unisa.edu.au/policies-and-procedures/codes/assessment-policies/.

Additional assessment requirements

There are no additional assessment requirements identified for this course.

Students with disabilities or medical conditions

Students with disabilities or medical conditions or students who are carers of a person with a disability may be entitled to a variation or modification to standard assessment arrangements. See Section 7 of the Assessment Policy and Procedures Manual (APPM) at: http://i.unisa.edu.au/policies-and-procedures/codes/assessment-policies/

Students who require variations or modifications to standard assessment arrangements should make contact with their Course Coordinator as early as possible in order to ensure that appropriate supports can be implemented or arranged in a timely manner.

Students can register for an Access Plan with UniSA Access & Inclusion Service. It is important to make contact early to ensure that appropriate support can be implemented or arranged in a timely manner. See the Access and Inclusion for more information: https://i.unisa.edu.au/students/student-support-services/access-inclusion/

Students are advised there is a deadline to finalise Access Plan arrangements for examinations. Further information is available at: http://i.unisa.edu.au/campus-central/Exams_R/Before-the-Exam/Alternative-exam-arrangements/

Deferred Assessment or Examination

Deferred assessment or examination is available for this course.

Special Consideration

Special consideration is available for this course.

Variations to assessment tasks

Details for which variation may be considered are discussed in section 7 of the Assessment Policy and Procedures Manual. Variation to assessment in unexpected or exceptional circumstances should be discussed with your course coordinator as soon as possible.

More information about variation to assessment is available in section 7 of the Assessment Policy and Procedures Manual. http://i.unisa.edu.au/policies-and-procedures/codes/assessment-policies/

Students with disabilities or medical conditions please refer to **Students with disabilities or medical conditions**.

Academic Integrity

Academic integrity is the foundation of university life and is fundamental to the reputation of UniSA and its staff and students. Academic integrity means a commitment by all staff and students to act with honesty, trustworthiness, fairness, respect and responsibility in all academic work.

An important part of practising integrity in academic work is showing respect for other people's ideas and being honest about how they have contributed to your work. This means taking care not to represent the work of others as your own. Using another person's work without proper acknowledgement is considered Academic Misconduct, and the University takes this very seriously.

The University of South Australia expects students to demonstrate the highest standards of academic integrity so that its degrees are earned honestly and are trusted and valued by its students and their employers. To ensure this happens, the University has policies and procedures in place to promote academic integrity and manage academic misconduct. For example, work submitted electronically by students for assessment will be examined for copied and un-referenced text using the text comparison software Turnitin http://www.turnitin.com.

It is an offence for any person or company to provide academic cheating services to students of Australian universities, irrespective of whether the service is provided by an Australian or overseas operator (see Tertiary Education Quality and Standards Agency Amendment (Prohibiting Academic Cheating Services) Bill 2019 - https://www.legislation.gov.au/Details/C2020A00078). “Academic cheating services” includes providing or undertaking work for students, where that work forms a substantial part of an assessment task.

More information about academic integrity and what constitutes academic misconduct can be found in Section 9 of the Assessment Policies and Procedures Manual (APPM): http://i.unisa.edu.au/policies-and-procedures/codes/assessment-policies/. The Academic Integrity Module explains in more detail how students can work with integrity at the University: https://lo.unisa.edu.au/mod/book/view.php?id=252142

Further Assessment Information

Late submissions for Continuous assessments and Assessment 2 (Presentation) that do not have an approved extension may incur a penalty at a rate not exceeding 10% per whole or part day late (including Saturday, Sunday and public holidays). The marks deducted will be equal to the penalty percentage applied to the total available marks (e.g. an original mark of 50/100 with a 10% penalty would result in a final mark of 40/100). Submissions that are more than 6 days late, without prior arrangement, will automatically incur a grade of F2. This does not apply to the examination, which instead follows the processes for deferred assessment or examination outlined in the APPM .

Assignment Cover Sheets should **not** be included with online submissions (note that assignment cover sheets are distinct from title pages which should be included where appropriate).

If you have any **issues with assessment submission**, please send a copy of your assessment via email to the course coordinator immediately with an explanation of the issue.

Action from previous evaluations

We value your feedback and will endeavour to implement suggestions wherever practical. Please provide any feedback you may have on course content, structure or any other matter to the course coordinator throughout the duration of the course.

Course Calendar

Study Period 5 - 2021

	Weeks	Topic
	12 - 18 July	Pre-teaching
	19 - 25 July	Pre-teaching
1	26 July - 1 August	Course Introduction & CIA Triad
2	02 - 8 August	Cryptography
3	09 - 15 August	Cybersecurity Attacks: Lifecycle and Motivations
4	16 - 22 August	Cyber Intrusions
5	23 - 29 August	Defence-in-Depth
6	30 August - 5 September	Social Engineering
7	06 - 12 September	Malware / Ransomware
8	13 - 19 September	Denial of Service
	20 - 26 September	Mid-break
	27 September - 3 October	Mid-break
9	04 - 10 October	Insider Threats
10	11 - 17 October	Data Exfiltration
11	18 - 24 October	Roles & Responsibilities
12	25 - 31 October	Guest Lectures
13	01 - 7 November	Course Review and Exam Information
	08 - 14 November	
	15 - 21 November	Exam week
14	22 - 28 November	Exam week