School of Computing and Engineering Technologies

Unit Outline

COS80013
Internet Security

Semester 1 2025

Please read this Unit Outline carefully. It includes:

PART A Unit summary

PART B Your Unit in more detail

PART C Further information

PART A: Unit Summary

Unit Code(s)		COS80013
Unit Title		Internet Security
Duration		One semester or equivalent
Total Contact Hours		48 hours
Requisites:		
	Pre-requisites	COS60004 Creating Web Applications OR COS60007 Creating Web Applications and Databases OR Admission into MA-ITPC1 - Master of Information Technology (Professional Computing) AND TNE60002 Network Administration OR COS70007 Data Communications and Security OR COS80021 Web Application Development OR TNE60006 Networks and Switching
	Co-requisites	Nil
	Concurrent pre-requisites	Nil
	Anti-requisites	Nil
	Assumed knowledge	Nil
Credit Points		12.5 credit points
Campus/Location		Hawthorn
Mode of Delivery		Blended
Assessment Summary		Research Project (Individual) 40% Applied Project (Individual) 40% Weekly labs (Individual) 10% Test (Individual) 10%

Aims

Students who complete this unit of study will understand the nature of security threats to IT systems. Students will also be aware of deficiencies in modern software systems and will understand how to manage the security of computer networks. Students will be familiar with the tools used by hackers and crackers and be aware of ways of identifying and rectifying security breaches and they will be able to collect digital evidence and understand the rules of evidence gathering.

Unit Learning Outcomes

Students who successfully complete this unit can,
ULO1: Evaluate security and privacy of networks and servers

ULO2: Develop management plans for system security
ULO3: Plan security audits with a focus on ICT ethics
ULO4: Understand social engineering concepts and assess system risks influenced by human behavior
ULO5: Utilize a range of security tools to solve complex cybersecurity problems
ULO6: Identify potential vulnerabilities through a solid understanding of network monitoring concepts
ULO7: Analyse and interpret logs and make recommendations on current Internet Security based on independent research

Graduate Attributes

The Swinburne Graduate Attributes describe the capability of our graduates to use knowledge, skills and behaviours to contribute to society meaningfully and positively. They include professional, self-directed learning and future-ready skills.
This unit contributes to the development of the following Swinburne Graduate Attributes,

1. **GA1 Communication - Verbal communication**

• Students develop their verbal communication skills through interactive workshops. They are required to discuss their project strategies, receive feedback, and engage in discussions, enhancing their ability to articulate ideas clearly and effectively.

2. **GA2 Communication - Communicating using different media**

• The unit involves implementing security strategies. Students learn to tailor their communication style to different digital platforms, effectively reaching and engaging their target audience.

3. **GA5 Digital Literacies – Information Literacy**

• In this unit, students are trained to critically evaluate and utilize information from a wide range of digital sources pertinent to cybersecurity. This includes identifying reliable sources of security updates, understanding threat intelligence reports, and using databases to research vulnerabilities and security breaches.

4. **GA6 Digital Literacies – Technical Literacy**

• The unit equips students with hands-on experience in using cybersecurity tools and technologies, such as intrusion detection systems, encryption tools, and vulnerability assessment software.
Other graduate attributes may be practised in the unit but are not formally taught as part of the unit content, nor incorporated within formal assessment.

Content

- Overview of network and computer security threats
- Physical and converged security
- Operating system
- Secure programming practices
- Port scanning, packet sniffing and intrusion detection
- Understanding and responding to security alerts
- Server technologies, risks and policies
- Vulnerability analysis and Audit
- Security models
- Authentication (identity, biometrics and digital signatures)
- Digital forensics
- ICT ethics and privacy

PART B: Your Unit in more detail

Unit Improvements

Feedback provided by previous students through the Student Survey has resulted in improvements that have been made to this unit. Recent improvements include:

- Updated teaching and learning materials and added recent technical progress
- Improved the assignment specification and added more supporting information
- Updated Assignment 1 to reflect more on technical aspects of learning

Teaching Staff

Name	Role	Room	Email / Teams	Consultation Times
Rory Coulter	Lecturer	-	rjcoulter@swin.edu.au	Refer to Canvas
Yasas Akurudda Liyanage Don	Lecturer /Tutor	EN505	yakuruddaliyanagedon@swin.edu.au	Refer to Canvas

- Professor Jun Zhang is the unit convenor for this unit

Learning and Teaching Structure

Category	Activity	Total Hours	Hours per Week	Teaching Period Weeks
Live Online	Lectures	12 hours	1 hours	Weeks 1 to 12
Online	Class	12 hours	1 hour	Weeks 1 to 12
In person	Workshop	24 hours	2 hours	Weeks 1 and 12

Week by Week Schedule

Week	Week Beginning	Teaching and Learning Activity	Student Task or Assessment
1	March 3	Lecture: Overview • Fundamental Concepts • Cyber Threats • Risk •Tactics, Techniques and Procedures Lab: Linux	Readings: Goodrich Chapter 1 Journal article 1 Listen: Security Now 1, 47, 50, 53, 57, 65. Risky Business 217. Reading: Information Security Manual (ISM)

2	March 10	Lecture: •Physical Security •Converged Security •Authentication •Social Engineering •Phishing and Pharming Attack Lab: Linux	Readings: Goodrich Chapter 2 Journal article 2 Listen: Security Now 211, 213, 137, 90, 94, 291; Risky Business 240, 163. 159, 129, 73, 70, 52, 51 Lab 1 due
3	March 17	Lecture: Operating System security •Operating System Security •Password •Buffer Overflow Attacks •Event, Audit, Sysmon, SE Linux Lab: Buffer overflows	Readings: Goodrich Chapter 3 Journal article 3 Listen: Security Now 39, 53, 54, 55, 78, 172, 174; Risky Business 152, 120 Lab 2 due
4	March 24	Lecture: Malware & Vulnerabilities •Malware Overview •Malware Analysis •Vulnerabilities •Vulnerability Management Lab: Malware, RATs and remote access	Readings: Goodrich Chapter 4 Journal article 4 Listen: Security Now 8, 9, 21, 22, 191, 193, 321, 353; Risky Business 67, 170, 169, 160, 17 Lab 3 due
5	March 31	Lecture: Network Security •Network Attacks •Firewall, IDS, IPS Lab: Denial of Service, tools	Readings: Goodrich Chapter 5, 6 Journal article 5 Listen: Security Now 25, 26, 27, 29, 195, 313, 319. Risky Business 11, 187, 188, 189 Lab 4 due

6	April 7	Lecture: Red, Purple & Blue Teams, Security Tools and Commands •Teams •SIEM •AV, EDR, XDR •Pen Test, Pen Test Interview Lab: Hack a site	Lab 5 due **Assignment 1 due**

7	April 14	Lecture: Intelligence •Intelligence Types •Threat Intelligence •Intelligence Functions •Espionage, Attackers **Lab: XSS, cookies**	Lab 6 due **Online Test in Lab**
Easter/Mid-Semester break - Thursday 17 April to Wed, 23 April. Split week			
8	April 28	Lecture: Web & Database Security •Web Security •Web Privacy •Dark Web •Cross-Site Scripting Attack (XSS) •Structured Query Language(SQL) Lab: Quiz test	Readings: Goodrich Chapter 7 Journal article 7 Security Now 85, 86, 87, 166, 168, 217, 219, 221, 225, 285. Risky Business 174
9	May 5	Lecture: Cryptography •Basic Scenario of Cryptography •Symmetric Key Cryptography •Public Key Cryptography •Hash Function •PGP/GPG (web of trust) & SSL & Digital Signature Lab: Crypto	Readings: Goodrich Chapter 8 Journal article 8 Listen: Security Now 125, 151, 179, 181, 183, 185, 195, 243. Risky Business 187, 197, 212 Lab 7 due

10	May 12	Lecture: Security Models & Frameworks •Security Models •Frameworks ISO •Mitre, NIST, E8 Lab: SQL injection	Lab 8 due
11	May 19	Lecture: Distributed- Application System, Privacy •App Dev & Testing •Fuzzing •E-mail & Spam •Privacy Lab: Forensics	Readings: Goodrich Chapter 9 Journal article 9 Listen: Security Now Risky Business 102 Lab 9 due
12	May 26	Lecture: Law and Order, GRC, Incident Response •Law, Critical Infra •Illegal Activities •GRC •Forensics •Incident Response	Lab 10 due
13	June 2		Assignment 2 due

Assessment

a) Assessment overview

Tasks and Details	Individual or Group	Weighting	Unit Learning Outcomes that this assessment task relates to	Assessment Due Date
1. Weekly Labs	Individual	10%	1-7	At the following lab session
2. Test	Individual	10%	1,2,3,4,7	Week 7
3. Research Project	Individual	40%	4,5,6,7	Week 6
4. Applied Project	Individual	40%	1-7	Week 13

Assessment Requirements	Details
b) Use of generative AI (genAI) in this unit	All assessments should be completed entirely without AI assistance.
c) Hurdle requirements	Aggregate 50% to pass the unit
d) Final assessment period	Final Practical Project need to be submitted to the Canvas by the due set during the final assessment period
e) Submission requirements	Assignments and other assessments are generally submitted online through the Canvas assessment submission system which integrates with the Turnitin . Please ensure you keep a copy of all assessments that are submitted. In cases where a hard copy submission is required an Assessment Cover Sheet must be submitted with your assignment. The standard Assessment Cover Sheet is available from the Submitting work webpage or www.swinburne.edu.au/studentforms/

f) Extensions and late submissions	Late Submissions - Unless an extension has been approved, late submissions will result in a penalty. You will be penalised 10% of your achieved mark for each working day the task is late, up to a maximum of 5 working days. After 5 working days, a zero result will be recorded.
g) Referencing	To avoid breaching academic integrity, you are required to provide references whenever you include information from other sources in your work and acknowledge when you have used Artificial Intelligence (AI) tools (such as ChatGPT). Further details regarding academic integrity are available in Section C of this document. Referencing conventions required for this unit are: IEEE/Harvard/ACM Helpful information on referencing can be found at http://www.swinburne.edu.au/library/referencing/
h) Groupwork guidelines	NA

Required Textbook(s)

The required textbook(s) can be purchased from bookshops and may be available through the Swinburne Library or.
http://bookshop.swin.edu.au
• Introduction to Computer Security, M T Goodrich and R Tamassia, Addison Wesley (Pearson), any edition

Recommended Reading Materials

Swinburne Library has a large collection of resources. Listed below are some references that will provide valuable supplementary information to this unit. It is also recommended that you explore other sources to broaden your understanding.

- Gray Hat Hacking, The ethical hacker's handbook 3rd. ed, A Harper [et al.], McGraw-Hill 2011
- Podcasts can be obtained from http://risky.biz , http://www.grc.com/SecurityNow.html and http://www.twit.tv
- Rory Coulter, Qing-Long Han, Lei Pan, Jun Zhang, Yang Xiang, “Data Driven Cyber Security in Perspective - Intelligent Traffic Analysis”, IEEE Transactions on Cybernetics, vol. 50, no. 7, pp. 3081-3093, 2020.
- The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition
- Practical Packet Analysis – Using Wireshark to Solve Real–World Network Problems 2e
- The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory

PART C: FURTHER INFORMATION

For further information on any of these topics, refer to Swinburne's Student webpage http://www.swinburne.edu.au/student/

Student behaviour and wellbeing

All students are expected to: act with integrity, honesty and fairness; be inclusive, ethical and respectful of others; and appropriately use University resources, information, equipment and facilities. All students are expected to contribute to creating a work and study environment that is safe and free from bullying, violence, discrimination, sexual harassment, vilification and other forms of unacceptable behaviour.

The Student Charter describes what students can reasonably expect from Swinburne in order to enjoy a quality learning experience. The Charter also sets out what is expected of students with regards to your studies and the way you conduct yourself towards other people and property.

You are expected to familiarise yourself with University regulations and policies and are obliged to abide by these, including the Student Academic Misconduct Regulations, Student General Misconduct Regulations and the People, Culture and Integrity Policy. Any student found to be in breach of these may be subject to disciplinary processes.

Examples of expected behaviours are:

- conducting yourself in teaching areas in a manner that is professional and not disruptive to others
- following specific safety procedures in Swinburne laboratories, such as wearing appropriate footwear and safety equipment, not acting in a manner which is dangerous or disruptive (e.g. playing computer games), and not bringing in food or drink
- following emergency and evacuation procedures and following instructions given by staff/wardens in an emergency response.

Canvas

You should regularly log on to the Swinburne learning management system, Canvas. You can access Canvas via the Student login webpage or https://swinburne.instructure.com/ Canvas is updated regularly with important unit information and communications.

Communication

All communication will be via your Swinburne email address. If you access your email through a provider other than Swinburne, then it is your responsibility to ensure that your Swinburne email is redirected to your private email address.

Academic Integrity

Academic integrity is about taking responsibility for your learning and submitting work that is honestly your own. It means acknowledging the ideas, contributions and work of others; referencing your sources and acknowledging the use of generative artificial intelligence;

contributing fairly to group work; and completing tasks, tests and exams without cheating. Artificial intelligence tools should only be used where approved by the Unit Convenor.

Swinburne University uses the Turnitin system, which helps to identify inadequate citations, poor paraphrasing and unoriginal work in assignments that are submitted via Canvas. Your Unit Convenor will provide further details.

Plagiarism, collusion, contract cheating, unauthorised file sharing, falsification, fabrication, manipulation or misrepresentation of information, reuse of previous work and non-compliance with instructions in an invigilated or non-invigilated assessment item are all breaches of academic integrity and treated as academic misconduct. Examples of breaches of academic integrity include, but are not limited to:

- submitting work as your own for assessment that has been fully or partially completed by a third party, either paid or unpaid
- using output from artificial intelligence tools (e.g. ChatGPT) in whole or part without acknowledgement and/or without the approval of the Unit Convenor
- using another person's work or ideas as though it is your own work, without appropriate attribution
- working closely with another student or group of students (either past or current), to submit for assessment, some or all of the other student or students' work as your own work
- sharing without permission of the Unit Convenor, Swinburne resources or other material related to assessment to an entity or document repository site
- creating, intentionally modifying or inventing information that is intended to be submitted as part of an assessment item
- using the whole or part of a computer program written by another person as your own without appropriate acknowledgement
- poorly paraphrasing somebody else's work
- using a musical composition or audio, visual, graphic and photographic work created by another person without acknowledgment
- enabling others to cheat, including letting another student copy your work or by giving access to a draft or completed assignment
- letting someone or something else impersonate you, or you impersonate someone else in an invigilated or non-invigilated assessment item
- accessing, obtaining and/or providing to others unauthorised materials relating to an invigilated or non-invigilated assessment item.

The penalties for academic misconduct can be severe, ranging from a zero grade for an assessment task through to exclusion from Swinburne. For further details, see https://www.swinburne.edu.au/student-login/academic-integrity/

Student support

Swinburne offers a range of services and resources to help you complete your studies successfully. Your Unit Convenor or studentHQ can provide information about the study support and other services available for Swinburne students. For further information, see the Current students web page.

Special consideration

If your studies have been adversely affected due to serious and unavoidable circumstances outside of your control (e.g. severe illness or unavoidable obligation), you may be able to apply for special consideration (SPC).

Applications for Special Consideration are submitted via the SPC online tool normally no later than 5.00pm on the third working day after the submission/sitting date for the relevant assessment component. See https://www.swinburne.edu.au/life-at-swinburne/student-support-services/special-consideration-assistance/

Note: Submitting fraudulent (fake or altered) medical certificates is considered misconduct and can lead to serious penalties from Swinburne. In addition, your doctor may report fraudulent medical certificates as a prosecutable offence under the Victorian Crimes Act.

AccessAbility Services

If you are a student with a disability, medical or mental health condition or you have significant carer responsibilities, you may require reasonable adjustments to fully access and participate in education. Swinburne's AccessAbility Services can develop an Education Access Plan (EAP) that includes the services and reasonable adjustments that you need.

It is recommended that you register with AccessAbility Services when you first commence your course but you can contact the service at any time during your studies to find out about reasonable adjustments. Contact Accessibility Services to discuss further.

Review of marks

An independent marker reviews all fail grades for major assessment tasks. In addition, a review of assessment is undertaken if your final result is between 45 and 49 or within 2 marks of any grade threshold.

You can ask the Unit Convenor to check the result for an assessment item or your final result. Your request must be made in writing within 10 working days of receiving the result. The Unit Convenor can discuss the marking criteria with you and check the aggregate marks of assessment components to identify if an error has been made. This is known as local resolution. If you are dissatisfied with the outcome of the local resolution, you can lodge a formal complaint.

Feedback, complaints and suggestions

In the first instance, discuss any issues with your Unit Convenor. If your concerns are not resolved or you would prefer not to deal with your Unit Convenor, then you can complete a feedback form. See https://www.swinburne.edu.au/corporate/feedback/

Advocacy

If you require assistance with any academic issues, University statutes, regulations, policies and procedures, you are advised to seek advice from an Independent Advocacy Officer at the Swinburne Student Association. Talking to an Advocacy Officer is free, independent and confidential. For more information and booking an appointment, please see https://www.swinburne.edu.au/current-students/student-services-support/advocacy/