

# Expectations



# Reality



1a. Introduction

Jin Hong  
[jin.hong@uwa.edu.au](mailto:jin.hong@uwa.edu.au)

# 1a. Introduction: outline

- ❖ Team
- ❖ Location
- ❖ Schedule
- ❖ Assessments
- ❖ Remember

# Team



Jin Hong  
Unit coordinator  
Room CS1.10  
[jin.hong@uwa.edu.au](mailto:jin.hong@uwa.edu.au)



Larry Huynh  
Lab Boss  
Does quantum computing stuff



Alian Haidar  
Lab facilitator  
Wrote your privacy lab



Jack Sun  
Lab facilitator  
UISS (~~UWA Hackers~~) President



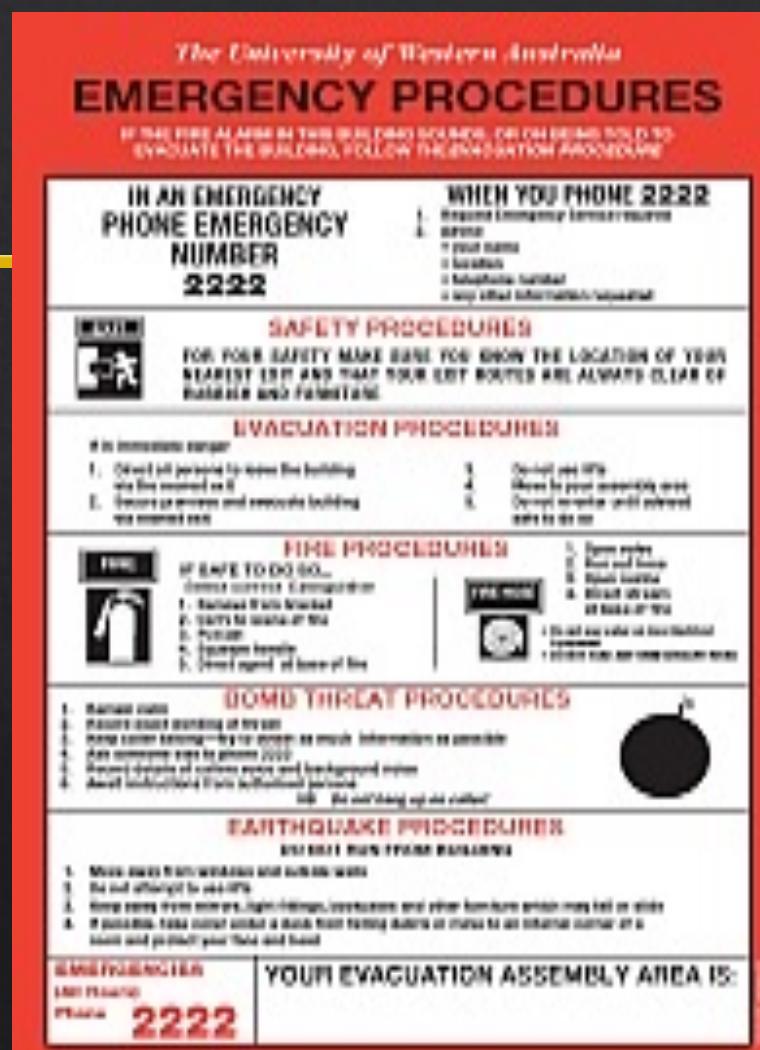
Muslim Gilani  
Lab facilitator  
Yet another ~~hacker~~ Cyber expert



Teaching Operations (team)  
Admin team  
Room Main reception  
[teachingops-team2@uwa.edu.au](mailto:teachingops-team2@uwa.edu.au)

# Emergency

- ❖ General emergency: call campus security at 6488 2222
- ❖ In super emergency: call emergency at 000
- ❖ In all buildings, we have an emergency procedure such as this picture ->
  - ❖ Please take a time and read it.
- ❖ For more details, please have a read through our emergency procedure for various potential incidents
  - ❖ <http://www.safety.uwa.edu.au/incidents-injuries-emergency/procedures>



# Location

---

- ❖ Lecture
  - ❖ Venue: Woolnough Lecture Theatre (GGGL 107)
  - ❖ Time: Mondays 11am – 1pm
- ❖ Labs
  - ❖ Lab 1: EZONE CENT 105 @ Tuesdays 9am – 11pm
  - ❖ Lab 2: EZONE CENT 209 @ Wednesdays 1pm – 3pm
  - ❖ Lab 2: EZONE CENT 209 @ Fridays 11am – 1pm
- ❖ Consultation
  - ❖ Office at Computer Science building room 1.10 – email to book a time

Changes will be announced (if any)

# Location

The screenshot shows the Microsoft Teams application interface. On the left, a sidebar menu includes options like Activity, Chat, Teams (selected), UWA Intra..., Calendar, Calls, OneDrive, Power BI, and Apps. The main area displays a team named "CITS2006" with a thumbnail image of a person and the title "Defensive Cybersecurity SEM-1 ...". Below this, under "Main Channels", are three channels: General, Facilitators, Lab discussion, and Project discussion. The "General" channel is currently selected, indicated by a blue underline. At the top right, there are tabs for General, Posts, Files, LMS, Library, and a plus sign. A search bar at the top right contains the placeholder "Search". On the far right, there is a decorative graphic of four stylized human avatars (two men and two women) with speech bubbles, and text encouraging conversation.

Let's get the conversation started

Try @mentioning a student or teacher to begin sharing ideas.

# Course overview: Term 1

Labs start first week!

Week	Lecture	Lab	Assessments
1	Intro + Defence overview	Lab 0: Background	
2	Cryptography	Lab 1: Hashing and Blockchain	
3	Privacy*	Lab 2: Privacy	
4	Access Control		Lab Quiz 1
5	Protocols and Tools	Lab 3: Access Control	
Study Break			

\*Privacy lecture will be available online due to Labour Day public holiday on Monday

# Course overview: Term 2

Week	Lecture	Lab	Assessments
6	Threat Intelligence	Lab 4: Protocols and Tools	
7	IDS		Lab Quiz 2
8	<b>ANZAC Day (no lecture)</b>	Lab 5: IDS	Project out
9	Security Modelling and Analysis	Lab 6: Risk Analysis	
10	Proactive Cybersecurity		Project demo
11	Security Management		Lab Quiz 3
12	Special Topic		Project demo

# Assessments

Assessment Item	When	Covers	Worth (total)
Lab Quizzes	Weeks 4, 7, 11	Topics up to the week	60% (20% each)
Project			
Stream 1: Group Project	Week 8	Various	40%

Please note, all dates are tentative and subject to change!

# How does the lab quiz work?

---

- ❖ During your scheduled lab time, you will be supervised by a lab facilitator to complete a timed lab quiz (~60 mins but can vary).
- ❖ You cannot receive mark if your attendance is not confirmed by the lab facilitator.
  - ❖ i.e., you must be supervised/invigilated by the lab facilitator to receive marks.
  - ❖ Attendance is required for all F2F students (unless a reasonable excuse is provided).

# How does the lab quiz work?

---

- ◊ We will be using a peer-marking system, where you will be formed into a group of 4 (or thereabout).
- ◊ For MCQ and written questions, marking keys will be provided.
- ◊ For Demo, you will be given 10~15 min slots to complete the demo.
- ◊ Marking keys will be provided for peer markers to use and submit the report.
- ◊ The peer markers will also provide feedback to the demonstrator including the mark range.
- ◊ Facilitators will be available for any moderations and review of the peer marking process.
- ◊ All submitted peer marks will be reviewed and moderated, and finalised marks will be uploaded to csmarks.
  - ◊ <https://secure.csse.uwa.edu.au/run/chapter0>

# Project

- 
- ❖ Details to be confirmed but this year I am thinking:
    - ❖ You will be put in a group
    - ❖ Part 1 (40%) : Design and implement a security feature based on given specs.
    - ❖ Part 2 (30%) : Evaluate and discuss implementation of other groups.
    - ❖ Part 3 (30%) : Individual reports for parts 1 and 2.
    - ❖ You will submit accompanying reports (group and individual) as well as doing Demo as required.
    - ❖ But TBC.

# Prerequisites and recommendations

---

- Prerequisites: CITS1003 and CITS1401 (or their equivalents)
- You will need to be familiar with Linux
- You will also need to study a bit about basic computer networking
  - Lab 0 will cover Linux and basic networking so don't panic.
- You may also use other programming languages other than Python as necessary.
  - But we'll keep this to minimal.
- You should also be familiar with basic discrete mathematics and number theory.

# Please note

---

- Lectures provide **theoretical** and **conceptual** understandings of the topics presented
  - But we will also do some practicals in the lectures as applicable
  - So, you should bring your laptop if you want to try them in class as well
- Labs and project provide **practical skills** of the topics presented
- The contents in Lectures, labs and project will be related, but they are all **INDEPENDENT** learning materials
  - i.e., you will be learning new things in each lecture, lab and project.

# Copyright notice

---

## Commonwealth of Australia

Copyright Regulations 1969

### WARNING

Materials in this unit (CITS3006 – Penetration Testing) have been reproduced and communicated to you by or on behalf of The University of Western Australia pursuant to Part VB of the *Copyright Act 1968* (**the Act**).

The material in this communication may be subject to copyright under the Act. Any further reproduction or communication of this material by you may be the subject of copyright protection under the Act.