
Welcome
Ласкаво просимо
Vitajte
Tervetuloa
Welkom
ברוך הבא
Dobro došli
مرحبا
Sveiki atvykę
Bun venit
Bem-vindo
Selamat datang
Bienvenido
Benvingut
Laipni lūdzam
Witamy
Добре дошли
환영
Добро пожаловать
Willkommen
Chào mừng
Vítejte
Velkommen
ようこそ
Καλώς ορίσατε
歡迎
Dobrodošli
Tervetuloa
Welkom
Bienvenue
Välkommen
Benvenuto
स्वागत
Maligayang pagdating
欢迎
Bienvenido
Maligayang pagdating
Vitajte

CYBR3000

Introduction to course

Dr Dan Kim

Associate Professor in Cybersecurity,
School of EECS
The University of Queensland, Australia
Homepage: https://researchers.uq.edu.au/researcher/23703

Course coordinators & lecturers

- Associate Prof. Dan Kim, PhD
  - Email: CYBR3000@eecs.uq.edu.au
  - Building/room: 78-440
  - Office hours: appointment by email.

- Associate Prof. David Ross, PhD
  - Email: CYBR3000@eecs.uq.edu.au
  - Building/room: 78-449
  - Office hours: appointment by email.

Course materials

- Lectures
  - Menu: Lecture
  - Lecture notes are on the Learn (blackboard ultra)
- Applied Classes - questions and answers
  - Menu: Course content
- Discussion:
  - Menu: Ed Discussion Board
- Recommended Resources
  - William Stallings & Lawrie Brown, Computer Security: Principles and Practice, (Global Edition), 4th Edition (3rd edition is fine).
  - Ross Anderson, Security engineering, 3rd Edition, https://www.cl.cam.ac.uk/~rja14/book.html
  - Computer & Internet Security: A Hands-on Approach, 2nd Edition
  - Mark Stamp, Information Security principles and practice, 2nd Edition.
  - Other resources and their information will be included on the lecture slides.

Assumed Background – please read them carefully!

- It is assumed that students have passed CSSE2310 (or a course with similar content).
- Students **WILL** require a sound understanding of operating systems principles, computer networking principles, programming (**proficiency in C and Python program language** is essential and assembly language is required), and program execution.
- This is strongly required prerequisite knowledge and will not be re-taught during this course.
- Students will also require a general computing background consistent with having completed two years of an undergraduate degree in Computer Science / Information Technology / Software Engineering or Digital Systems Electrical Engineering.
- Students must understand TCP/IP basics, packet encapsulation, connection-oriented and connectionless protocols, program counters, stack and heap operations, memory layout, bits, bytes, nibbles, words, big-endian, little-endian, bitwise logic operations, and also be able to convert between decimal, binary and hexadecimal numbers.

Lecture and Applied Classes

- Attend lecture and participate in-class/online activities.
- No Applied Classes in the first week.
- There will be Applied Classes in weeks 2-11 (this is subject to change); please attend your allocated slot; you will solve Applied Classes questions.

Assessment items

- Online Weekly Quizzes, 10%
- Assignment, 35%
- On-campus paper exam final exam, 55%

Weekly Quizzes

- Weekly quiz is on **Ed Discussion -> Lessons**
- Weekly online quizzes will be due every Tuesday at 5:00 pm, starting from week 2.
- That is, the Week 1 quiz is due 5:00 pm the following Tuesday (Week 2), through to, the Week 12 quiz is due 5:00 pm the following Tuesday (Week 13).
- 12 quizzes will be made available in total. The answers are provided on the platform immediately on the due date, so no extensions are possible and there is an immediate 100% late penalty. **Missed (or late) submissions are included in the calculations as zero marks.**
- **You can submit it once; please make sure to complete your submission.**
- To accommodate unforeseen circumstances such as illness, your mark will be based on your best 10 out of the 12 possible submissions. All weeks are calculated of equal value, no matter how many marks are in any particular weekly quiz.
- Quizzes will usually cover topics from the previous week or two of classes but may cover topics from any previous week and/or may require students to do some research or reading beyond the class notes. Students are expected to take the quiz individually and on their own time and these weekly quizzes are designed to keep students up to date with the week by week teaching material. Each quiz must be explicitly submitted by the due date (i.e. quizzes are not auto-submitted).
- Artificial Intelligence (AI) and Machine Translation tools are permitted to be used in the quizzes, but they are not required to be used and not recommended to be used as they may inhibit learning.
- **No extension is allowed for Quizzes.**

Assignment

- Information security hands-on labs.
- You are required to complete hands-on labs and the results are to be submitted to the submission site via the link on Blackboard.
- Complete tasks for the assignment will be detailed on the handout for that assessment item.

Assignment (cont.)

- **The content of the assignments will be NOT be fully covered in Lecture in depth but only covered by the applied classes and help sessions for the assignments.**

- It is not guaranteed to cover the topics in assignments in advance, the assignments release dates are not following the course lecture schedule, you will have to expect that the tutorials/assignments help session(s) will cover the assignment topics, not by lectures.

Assignment (cont.)

- Referencing and Use of AI
  - Note that the assignment is to be worked on individually and must be your own work except where the use of code written or provided by other entities (teaching staff, Linux man pages, AI tools, etc.) is explicitly permitted by the assignment specification. Artificial Intelligence (AI) and Machine Translation (MT) are emerging tools that may support students in completing this assessment task. Students may appropriately use AI and/or MT in completing this assessment task. Students must clearly reference any use of AI or MT in each instance. You must follow the referencing requirements set out in the assignment specification.
  - A failure to reference generative AI or MT use may constitute student misconduct under the Student Code of Conduct.
  - Assignments with no academic merit (e.g. entirely written by AI, with insufficient content of your own academic value) will be awarded a mark of zero.
- Programming Assignment Interviews
  - Teaching staff will conduct interviews with a subset of students about their submissions for the purpose of establishing genuine authorship. If you write your own code, you have nothing to fear from this process. If you legitimately use permitted code from other sources (following the usage/referencing requirements in the assignment specification) then you are expected to understand that code.
- Deferral or extension
  - You may be able to apply for an extension.
  - The maximum extension allowed is 28 days. Extensions are given in multiples of 24 hours.
- Late submission
  - A penalty of 10% of the maximum possible mark will be deducted per 24 hours from time submission is due for up to 7 days. After 7 days, you will receive a mark of 0.
- More details in the course profile.

Final exam – closed book

- It is closed book and not allowed to access to any resources in Internet and digitally stored information (e.g., laptop, smart devices).
- Questions: short, long, problem solving questions from course materials in lecture/applied classes.
- The schedule of the final exam will be centrally managed by the university.
- University approved calculator is allowed to use.
- On-campus paper based exam
- The past exam questions are available

Tentative Schedule

- **Note that this is a tentative schedule and the schedule/topic is subject to change.**

- Some topics could be covered more or less so that some lecture may be longer or shorter.

- The number of the tutors can be reduced/increased based on the progress of the lecture and other circumstances.

Tentative topics
the schedule is subject to change.

- Section 1 (mostly covered by Dan)
  - Cybersecurity overview
  - Security management
  - Vulnerability Assessment
  - Threat model
  - Cyber-Attacks
  - Firewalls
  - Intrusion Detection
- Section 2 (mostly covered by David)
  - Crypto tools
  - PKI
  - SSL
  - IPSec

Questions

1. What is your name, favourite food, a place to recommended to visit?

2. What do you expect from this course?

3. Any other questions?