THE UNIVERSITY OF AUCKLAND
Te Whare Wānanga o Tāmaki Makaurau
NEW ZEALAND

BUSINESS SCHOOL

Course Outline 2017
INFOSYS 727: ADVANCED INFORMATION SECURITY (15 POINTS)

Semester 1 (1173)

Course Prescription

Focuses on technical security issues of the systems used in today's information technology applications. Explores the practical issues of identification and authentication, security of operating systems, cryptography, disaster recovery and models. Managerial aspects of information security issues as well as legal and ethical issues arising from protecting computer files both from a New Zealand and global perspective wil be addressed. The course follows the content of CISSP certification. This course covers curriculum of the Certified Information Systems Security Professional (CISSP), being the world most known information security professional certification.

Goals of the Course

This course presents technical and organisational arrangements of making information systems more secure. This process starts with defining the proper approach to setting up a security system, which are culminates with development of security policy. Basic components of security system will be discussed: firewalls, intrusion detection systems, encryption, security assessment, and security standards. Typical defences against viruses and other malicious software will be presented. Phenomena of cyber terrorism and cyber warfare will also be covered.

Learning Outcomes

By the end of this course it is expected that the student will be able to:

1. display familiarity with the major concepts and tools in current information security theory and practice like:
   a. the basic information security concepts (security protocols, human-computer interfaces, access control, cryptography and distributed systems issues);
   b. developmental, managerial and audit issues including the review of the related law, evidence collection and security policies;
2. demonstrate critical and creative thinking in being able to formulate and justify appropriate recommendations and/or solutions to a information security problem;
3. exhibit improved information literacy skills in being able to source, evaluate, and summarise appropriate information on a given subject or topic in information security domain.

Content Outline

Session	Topic
1	Course introduction, Basic hardware and software
2	Cryptography
3	Information Security and Risk Management Access control
4	Application Security
5	Business Continuity and Disaster Recovery Planning
6	Legal, Regulations, Compliance and Investigations

7	Electronic and information warfare
8	Operations Security
9	Physical and Environmental Security
10	Security Architecture and Design
11	Telecommunication and Network Security
12	Ten Domains of CISSP Security, Course review

Note: the session length is approximately one week, topic is a subject of possible changes.

Learning and Teaching

This course will be offer on the city campus a variety of teaching approaches will be use including lectures, class discussions, labs, written assignments and presentations. The weekly meetings will last three hours. Students are expected to use at least six additional hours each week in reading and preparing for the class. Active participation is essential, and students will be expect to master material assigned in readings, presented in class lectures, discussions, and presentations.

Teaching Staff

Dr. Lech J. Janczewski
Associate Professor
Office: OGGB Room 480
Tel: 923 7538
Email: lech@auckland.ac.nz

Tutor:
Farzan Kolini
Email: f.kolini@auckland.ac.nz

Laboratories:

Subject of possible changes, starting at the third week of the semester.

1. Cryptography I
2. Cryptography II
3. Steganography
4. Computer forensic
5. Firewalls
6. Linux Security essentials
7. WEB Goat I
8. WEB Goat II
9. Lab assessment test

Learning Resources

- Course will follow the textbook: P. Gregory, CISSP Guide to Security Essentials, Course Technology, second edition, 2015, ISBN 978-1-285-06042-2

  Other useful books:

- M. Whitman and H. Mattord. Principles of Information Security, Thomson - Course Technology, 2014, Fifth Edition
- L. Janczewski, W. Caelli, Cyber Conflicts and Small States, Ashgate, ISBN 978-1-4724-5219-1
- Software used in lab: Provided by Instructor
- Lectures notes distributed via Canvas
- Links to related publications in newspapers, magazines and journals will be provided from time to time**.**

- Students are required to complete the prescribed readings and be fully prepared to contribute to the in-depth discussions.

Assessment

50% Coursework including:

- Midterm Test 10%
- Lab 20%
- Group project 20%

50% Final exam

The broad relationship between these assessments and the course learning outcomes is as follows:

Learning Outcome	Group Project	Test	Labs	Final Exam
1a		X	X	X
1b		X	X	X
2	X			X
3	X		X	X

Inclusive Learning

Students are urged to discuss privately any impairment-related requirements face-to-face and/or in written form with the course convenor/lecturer and/or tutor.

Student feedback

- Students will be asked to provide twice the semester evaluation of the course.