SUBJECT OUTLINE

41900 Security Fundamentals

Course area	UTS: Engineering
Delivery	Spring 2019; City
Subject classification	ICT Engineering program
Credit points	6cp
Requisite(s)	31268 Web Systems OR 48410 Introduction to ICT Engineering OR 31270 Networking Essentials OR 48720 Network Fundamentals OR 48721 Strategic e-Business Technologies OR 41092 Network Fundamentals
Result type	Grade and marks

Attendance: 3hpw, on campus
Recommended studies: Foundation Mathematics or equivalent

Subject coordinator

Dr. Ashish Nanda
Room: CB11.08.403
Email: Ashish.Nanda@uts.edu.au
Consultation Hours: Tuesday, 1.00PM - 2.00PM, CB11.05.300, Learning Precinct
The Subject Coordinator can be contacted by email if you have matters of a personal nature to discuss, e.g., illness, study problems, group problems, group re-assignment, or a request for an appointment outside the given consultation hours.

Teaching staff

Lecturer:
Dr. Ashish Nanda
Room: CB11.08.403
Email: Ashish.Nanda@uts.edu.au
Tutors:
Firas Al-Doghman
Email: Firas.al-doghman@uts.edu.au
If you wish to discuss your questions or need further help with understanding concepts in this subject, please see the tutor during the tutorial, or contact them via email.

Subject description

Security is a major issue for enterprises, with breaches leaving them vulnerable to legal sanctions, financial loss or reduced customer confidence. This subject introduces students to modern security issues and technologies by considering various aspects, from security principles and policies, to network and system security, as well as intrusion detection and cyber security. Students learn and apply programming skills to implement secure communications while demonstrating professional practice in a group project.

Subject learning objectives (SLOs)

Upon successful completion of this subject students should be able to:

1. Explain the major theories and principles of information security through examination of the mathematics behind prominent encryption algorithms.
2. Identify programmatic flaws which commonly produce unintended outcomes by examining and exploiting flawed software routines.

3. Implement secure protocols and techniques to prevent data interception and modification by modifying and improving provided software.
4. Discuss the potential impact of evolving cryptographic techniques on contemporary security protocols by reviewing recent literature.
5. Differentiate between acceptable and unacceptable aspects of system design that affect or compromise security principles by assessing code.
6. Work as an effective member of a software development team while undertaking a software development project.

Course intended learning outcomes (CILOs)

This subject also contributes specifically to the development of the following faculty Course Intended Learning Outcomes (CILOs) and Engineers Australia (EA) Stage 1 competencies:

- Apply systems thinking to understand complex system behaviour, including interactions between components and with other systems (social, cultural, legislative, environmental, business, etc.) (A.5)
- Identify and apply relevant problem-solving methodologies (B.1)
- Design components, systems and/or processes to meet required specifications (B.2)
- Apply decision-making methodologies to evaluate solutions for efficiency, effectiveness and sustainability (B.4)
- Implement and test solutions (B.5)
- Demonstrate research skills (B.6)
- Identify and apply relevant project management methodologies (E.3)

Teaching and learning strategies

This foundation subject consists of three face-to-face hours per week.

- A weekly one hour lecture
- A two hour of lab
  This will be a chance for students to form project groups and learn some basic programming skills. Groups are expected to work together for the whole two hour lab session every week and obtain project guidance from the tutor.
- Self-organised group meetings
  Groups should meet up for at least two hours per week in addition to the two hour class time to collaborate on the project and coordinate efforts on the project.

It is the responsibility of the student to check UTSOnline regularly and dedicate time to learning and development outside of class. Lectures and lab sessions are compulsory. They are supported by a series of slides, practical exercises, and additional readings. All materials and additional readings are examinable, unless explicitly stipulated otherwise during the lecture.
Programming:
If students are not familiar with programming, they will be provided with the opportunity and tools to learn during the beginning of the subject. Students are then expected to apply this skill by modifying an existing computer program. The ability to write code is essential for completion of the project, but not necessary for the final examination.
Active Learning:
The primary project for this subject involves group programming. Students must prepare for tutorials/labs to work effectively as part of a group, completing administrative, project management, and programming tasks prior to attending face-to-face sessions. Groups are expected to meet both inside and outside of class time to understand the basic workings of peer-to-peer communication by examination of example code. Groups must then improve the security of communication by implementing secure protocols. Basic project and group management skills will be essential for effective collaboration. Students will be asked individually to provide feedback on the code modifications made by other groups online.

Program

Week/Session	Dates	Description

1	22 Jul	**Lecture: Introduction to Information Security** Subject introduction information available at UTSOnline. Also, you are expected to pre-read/view material available at UTSOnline. **Notes:** **Lab/Tutorial:** Activities will start from Week 2
2	29 Jul	**Lecture: Number Theory** **Notes:** **Lab/Tutorial:** Material will be made available on UTSOnline
3	5 Aug	**Lecture: Hash Functions and Ciphers** **Notes:** **Lab/Tutorial:** Material will be made available on UTSOnline
4	12 Aug	**Lecture: Pseudo Random Number Generators & Block Ciphers** **Notes:** **Lab/Tutorial:** Material will be made available on UTSOnline **Assessment: Project Part-1** Introduction and Overview
5	19 Aug	**Lecture: Symmetric Key Cryptography & Key Management** **Notes:** **Lab/Tutorial:** Material will be made available on UTSOnline **Mini-Quiz:** Sample quiz available on UTSOnline with feedback
6	26 Aug	**Lecture: Asymmetric Key Cryptography** **Notes:** **Lab/Tutorial:** Material will be made available on UTSOnline **Assessment: Quiz 1** (To take place during Lab Session)
7	2 Sept	**Lecture: Authentication** **Notes:** **Lab/Tutorial:** Material will be made available on UTSOnline

StuVac	9 Sept	**Mid-Session StuVac** **Notes:** **No Lecture/Lab Activities**
8	16 Sept	**Lecture: Digital Signatures** **Notes:** **Assessment: Project Part-2** Introduction and Overview **Assessment: Project Part-1 Due** (Will be marked during Tutorial)
9	23 Sept	**Lecture: Security Protocols** **Notes:** **Lab/Tutorial:** Material will be made available on UTSOnline **Assessment: Quiz 2** (To take place during Lab Session)
10	30 Sept	**Lecture: Confidentiality & Integrity** **Notes:** **Lab/Tutorial:** Material will be made available on UTSOnline
11	7 Oct	**Lecture: Cryptocurrencies & Blockchain** **Notes:** **Lab/Tutorial:** Material will be made available on UTSOnline
12	14 Oct	**Final Exam Information** **Notes:** **Assessment: Project Part-2 Due** (Will be marked during Tutorial)

Assessment

Assessment task 1: Quiz 1 & 2

Intent: The Quizzes are designed to motivate continuous learning, analysis and the recall of the technical knowledge relevant to the subject concepts.

Objective(s): This assessment task addresses the following subject learning objectives (SLOs):

1, 2, 3, 4 and 5

This assessment task contributes to the development of the following course intended learning outcomes (CILOs):

B.1

Type: Quiz/test

Groupwork: Individual

Weight: 20%

Task: Two in-class quizzes will take place during the labs to ensure that students are keeping up with the lecture material. Each quiz will cover all lecture material that precedes it.

Length: Approx. 30 minutes in duration each

Due: Quiz 1 is held in week 6 & Quiz 2 is held in week 9. As all quizzes are held within the student's elected tutorial times, there is no excuse for student to claim unavailability to attend the quiz. Re-sits will not be permitted.
See also Further information.

Criteria linkages:

Criteria	Weight (%)	SLOs	CILOs
Correctness of solutions	100	1, 2, 3, 4, 5	B.1

SLOs: subject learning objectives
CILOs: course intended learning outcomes

Further information: Weighting: 20% (i.e., each quiz is worth 10%)

The feedback to the quizzes will be given to students by their tutor normally one week after the quiz. It is important for students to consult their tutor and to understand the area they need to improve on.

Assessment task 2: Group Project

Intent: Give students the opportunity to implement the theory gained during lectures and their own research, by designing and implementing secure algorithms and protocols.

Objective(s): This assessment task addresses the following subject learning objectives (SLOs):

1, 2, 3, 4, 5 and 6

This assessment task contributes to the development of the following course intended learning outcomes (CILOs):

.2, A.5, B.2, B.4, B.5, B.6 and E.3

Type: Project

Groupwork: Group, individually assessed

Weight: 40%

Task: A group of students will undertake a programming project to implement secure algorithms using a provided template. Students will be required to research appropriate techniques outside of class while some concepts will be covered in the lectures.
As programming fundamentals is a core subject for all students enrolled, and an essential competency to operate in the IT industry, support and opportunities will be provided to students who are new to programming, but it is the responsibility of the student to ensure they are sufficiently competent.
Furthermore, this subject is not focused on programing techniques. The marks will be given entirely based on the correctness or the functionality.
The software project is due in multiple parts, which will be released in weeks 4 and 8, and is due in

weeks 8 and 12.
Parts that are due:

- Part 1 - 20% - Week 8
- Part 2 - 20% - Week 12

See the assignment specification sheet for more details.

Length: Group work is due in two parts. Project will run from weeks 4 to 12.

Due: Part 1 (20%): Week 08 (09:00 AM, 06 May 2019). Part 2 (20%): Week 12 (09:00 AM, 03 June 2019). See also Further information.

Criteria linkages:

Criteria	Weight (%)	SLOs	CILOs
Program Completeness and correctness	50	1, 2, 3, 4, 5, 6	A.5, B.2, B.4, B.5, B.6, E.3
Additional analysis and innovation	20	1, 2, 3, 4, 5, 6	A.5, B.2, B.4, B.5, B.6, E.3
Well documented report	10	1, 2, 3, 4, 5, 6	A.5, B.2, B.4, B.5, B.6
Ability to answer questions during the demo day (individual)	20	1, 2, 3, 4, 5	A.5, B.2, B.4, B.5

SLOs: subject learning objectives
CILOs: course intended learning outcomes

Further information: Although this is a group assignment, individual knowledge and familiarity of the project is essential. A significant portion of the marks will still be rewarded individually. As this is a group assignment, except the extreme scenarios, where every member suffers from misadventure simultaneously, no extensions can be granted to any groups without a penalty. The project is to be marked within three weeks from its due date, the students are able to collect the feedback from the subject co-ordinators or the tutors.

Assessment task 3: Exam

Intent: The exam will explore the extent of students' knowledge and understanding of key and current standards, applications, and technologies presented during the lectures. The format will be similar to the quizzes, however it will require a deeper understanding of the content than the quizzes. It will not involve programming.

Type: Examination

Groupwork: Individual

Weight: 40%

Task: The exam will be restricted open book exam. Students are permitted to bring one double side A4 page of notes into the examination room.

The format of the exam will be similar to the quizzes, however it will require a deeper understanding of the content than the quizzes. It will not involve programming.

Length: 2 hours

Due: UTS Exam period

Assessment feedback

You will receive feedback for the early assessments, including Quiz 1 & 2.

Examination material or equipment

1. The final exam is restricted open book: Students are permitted to bring one double side A4 page of notes into the examination room.
2. The Quiz tests are closed book computer based: No materials are allowed.

Minimum requirements

In order to pass the subject, a student must achieve an overall mark of 50% or more.

Required texts

There is no prescribed textbook for this subject.

Recommended texts

William Stalling, Cryptography and Network Security, 4th Edition

William Stalling, Network Security Essential, 5th Edition

Matt Bishop, Introduction to Computer Security

Mark Ciampam Security+ Guide to Network Security Fundamentals, 4th Edition

Other resources

- Students must have a valid login to UTSOnline and be registered for 41900 Fundamental of Security on UTSOnline.
- If you do not have a valid login to UTSOnline you have to contact ITD helpdesk on 9514 2222.
- UTSOnline will be used as the major means of communication between subject co-ordinator, teaching staffs and students.
- Any change in schedule will be updated in UTSOnline.
- It is the responsibility of the student to read the UTSOnline regularly.
- UTSOonline will also be used to provide reference websites and other information.

Graduate attribute development

For a full list of the faculty's graduate attributes and EA Stage 1 competencies, refer to the FEIT Graduate Attributes webpage.

Assessment: faculty procedures and advice

Extensions

When, due to extenuating circumstances, you are unable to submit or present an assessment task on time, please contact your subject coordinator before the assessment task is due to discuss an extension. Extensions may be granted up to a maximum of 5 days (120 hours). In all cases you should have extensions confirmed in writing.

Special consideration

If you believe your performance in an assessment item or exam has been adversely affected by circumstances beyond your control, such as a serious illness, loss or bereavement, hardship, trauma, or exceptional employment demands, you may be eligible to apply for Special Consideration.

Late penalty

Work submitted late without an approved extension is subject to a late penalty of 20 per cent of the total available marks deducted per calendar day that the assessment is overdue (e.g. if an assignment is out of 40 marks, and is submitted (up to) 24 hours after the deadline without an extension, the student will have eight marks deducted from their awarded mark).

For some assessment tasks a late penalty may not be appropriate – these are clearly indicated in the subject outline. Such assessments receive a mark of zero if not completed by/on the specified date. Examples include:

1. weekly online tests or laboratory work worth a small proportion of the subject mark, or
2. online quizzes where answers are released to students on completion, or
3. professional assessment tasks, where the intention is to create an authentic assessment that has an absolute

submission date, or
4. take-home papers that are assessed during a defined time period, or
5. pass/fail assessment tasks.

Querying marks/grades and final results

If a student disagrees with a mark or a final result awarded by a marker:

- where a student wishes to query a mark, the deadline for a query during teaching weeks is 5 working days from the date of the return of the task to the student
- where a student wishes to query a final examination result, the deadline is 5 working days from the official release of the final subject result.

Further information can be found at the current students Results page.

Academic liaison officer

Academic liaison officers (ALOs) are academic staff in each faculty who assist students experiencing difficulties in their studies due to: disability and/or an ongoing health condition; carer responsibilities (e.g. being a primary carer for small children or a family member with a disability); and pregnancy.

ALOs are responsible for approving adjustments to assessment arrangements for students in these categories. Students who require adjustments due to disability and/or an ongoing health condition are requested to discuss their situation with an accessibility consultant at the Accessibility Service before speaking to the relevant ALO.

The ALO for undergraduate students is:

Chris Wong
telephone +61 2 9514 4501

The ALO for postgraduate students is:

Dr Nham Tran
telephone +61 2 9514 4468

Statement about assessment procedures and advice

This subject outline must be read in conjunction with the policy and procedures for the assessment for coursework subjects.

Statement on copyright

Teaching materials and resources provided to you at UTS are protected by copyright. You are not permitted to re-use these for commercial purposes (including in kind benefit or gain) without permission of the copyright owner. Improper or illegal use of teaching materials may lead to prosecution for copyright infringement.

Statement on plagiarism

Plagiarism and academic integrity

At UTS, plagiarism is defined in Rule 16.2.1(4) as: 'taking and using someone else's ideas or manner of expressing them and passing them off as ... [their] own by failing to give appropriate acknowledgement of the source to seek to gain an advantage by unfair means'.

The definition infers that if a source is appropriately referenced, the student's work will meet the required academic standard. Plagiarism is a literary or an intellectual theft and is unacceptable both academically and professionally. It can take a number of forms including but not limited to:

- copying any section of text, no matter how brief, from a book, journal, article or other written source without duly acknowledging the source
- copying any map, diagram, table or figure without duly acknowledging the source
- paraphrasing or otherwise using the ideas of another author without duly acknowledging the source
- re-using sections of verbatim text without using quote marks to indicate the text was copied from the source (even if a reference is given).

Other breaches of academic integrity that constitute cheating include but are not limited to:

- submitting work that is not a student's own, copying from another student, recycling another student's work,

recycling previously submitted work, and working with another student in the same cohort in a manner that exceeds the boundaries of legitimate cooperation
- purchasing an assignment from a website and submitting it as original work
- requesting or paying someone else to write original work, such as an assignment, essay or computer program, and submitting it as original work.

Students who condone plagiarism and other breaches of academic integrity by allowing their work to be copied are also subject to student misconduct Rules.

Where proven, plagiarism and other breaches of misconduct are penalised in accordance with UTS Student Rules Section 16 – Student misconduct and appeals.

Avoiding plagiarism is one of the main reasons why the Faculty of Engineering and IT is insistent on the thorough and appropriate referencing of all written work. Students may seek assistance regarding appropriate referencing through UTS: HELPS.

Work submitted electronically may be subject to similarity detection software. Student work must be submitted in a format able to be assessed by the software (e.g. doc, pdf (text files), rtf, html).

Further information about avoiding plagiarism at UTS is available.

Retention of student work

The University reserves the right to retain the original or one copy of any work executed and/or submitted by a student as part of the course including, but not limited to, drawings, models, designs, plans and specifications, essays, programs, reports and theses, for any of the purposes designated in Student Rule 3.9.2. Such retention is not to affect any copyright or other intellectual property right that may exist in the student's work. Copies of student work may be retained for a period of up to five years for course accreditation purposes. Students are advised to contact their subject coordinator if they do not consent to the University retaining a copy of their work.

Statement on UTS email account

Email from the University to a student will only be sent to the student's UTS email address. Email sent from a student to the University must be sent from the student's UTS email address. University staff will not respond to email from any other email accounts for currently enrolled students.