Security Stream for Computer Science

Compulsory
COMP3441 Security Engineering
or
COMP6442 Extended Security Engineering

Electives
and three electives drawn from the elective list (below)

COMP4442 -- Advanced Computer Security
COMP6443 – Web Application Security and Testing
COMP6444 – Extended Web Application Security and Testing
COMP6445 – Digital Forensics
COMP6446 – Extended Digital Forensics and Incident Response
COMP6447 – System and Software Security Assessment
COMP6448 – Security Engineering Masterclass
COMP6450 – Security Engineering Professional Practice
COMP9337 – Securing Wireless Networks
COMP9447 – Security Engineering Workshop
MATH3411 – Information, Codes and Ciphers

New Security Courses

- COMP6442 Extended Security Engineering

  An extended version of the current 3441 Course. Runs in parallel with 3441 but has an additional hour of lecture/week on reverse engineering machine code and malware analysis.

- COMP6443/4 – Web Application Security and Testing/ Extended

  New course. Secure web design and pen testing.

- COMP6445/6 – Digital Forensics/ Extended

  New course. Forensics and Incident Response.

- COMP6447 – System and Software Security Assessment

  New course. Content currently partially covered in 9447, 9447 coverage restored to original intent and matching name.

- COMP6450 – Security Engineering Professional Practice

  New course. Cyber professional practice, law and ethics.

- COMP6448 – Security Engineering Masterclass

  New Course. Masterclasses led by visiting experts. Run when experts are visiting.

COMP6442 Extended Security Engineering

An extended version of the current 3441 Course. Runs in parallel with 3441 but has an additional hour of lecture/week on reverse engineering machine code and malware analysis.

Justification
Some students take the basic version of this course, COMP3441, as an interest elective, some want to specialise in cyber security. There is a great interest in students outside of CSE taking 3441 to gain cyber literacy. Splitting into extended/basic versions allows the technical content to be taken by students with an interest (by taking this course 6442) and means non technical students can still take the 3441. The two coruses are identical and run at the same time except for one extra hour per week of lectures and additional formative assessments on the additional topics (see coverage below) and an additional final exam paper.

Coverage
Reversing x86 machine code into C/C++.
Malware reversing and analysis.

Assessments
as for 3441 plus additional weekly formative assessment activities (non compulsory) – quizzes, puzzles.

Resource Implications
The reversing lectures will be recorded in first offering so after the first offering the resource requirements will be as for 3441.

COMP6443/4 – Web Application Security and Testing/ Extended

Justification
Web applications are currently the predominant source of software vulnerabilities exploited in cyber attacks. There is a growing need and growing demand for web programmers to be security aware. This is likely to be a popular course for postgrads and those taking courses for industry PD.

The extended course will also cover the practice of penetration testing. There is a national and growing shortage of properly skilled pen testers. About half of our graduates who take jobs in cyber security initially work as pen testers.

Prerequisites
co-requisites: COMP3441 or COMP6442 or COMP9321.

Coverage
Top Web vulnerabilities
Cross site scripting
Browser security model and weaknesses
Injection attacks
DNS
Man in the middle
Data leakage
Spoofing
UI and Social vulnerabilities
Assurance and Testing
Standards

+ Extended:
terms of engagement
legal business and ethical issues
reporting
red teaming
remote testing
on-site testing
reporting and communicating effectively

Assessments
Weekly remote labs
Portfolio

Extended course: Pen test project and presentation to “client”

Resource Implications
Lecture 2 hours/week
Supervised Tutorial/Lab 1 hour/week
Resources to create online labs (met by CBA funding)

Extended version: one additional hour/week lecture

Text
Web Application Hackers Handbook (2nd ed)

COMP6445/6 – Digital Forensics/ Extended

Justification
This course addresses the skills and knowledge needed by first responders to a discovered cyber breech, as well as law enforcement and criminal justice.

Prerequisites
COMP3441 and at least one of COMP3231/9201/3891/9283.

Coverage
Memory Forensics
Disc Forensics
Network Forensics
Devices
Stealth Techniques
Anti-forensics
Forensic Practice (chain of custody, records etc)
Logging

+ Extended:
Malware techniques
Malware detection
CERTs
Principles of Incident Response

Assessments
6 lab assessments (in pairs)
Portfolio
Final Theory and Practical Exam.

+Extended course: Malware detection project

Resource Implications
Lecture 2 hours/week
Supervised Tutorial/Lab 2 hour/alternate weeks
Resources to create online lab activities (met by CBA funding)

+Extended course: one additional hour/week lecture, one additional hour lab/week

Text
The Shell coders Handbook

COMP6447 – System and Software Security Assessment

Justification
This course looks at cyber attack and defence. Students learn how to assess and identify vulnerabilities and how vulnerabilities are exploited. Students from this course will engage in war games competitions,

Prerequisites
COMP6442

Coverage
Vulnerability classes
Source code auditing
Fuzzing
Security Bugs
Software Security Assurance
Taint Analysis
Memory Corruption
Overflows
Return Oriented Programming

Assessments
Weekly war games
War game creation
Portfolio
Final Practical Exam.

Resource Implications
Lecture 2 hours/week
Tutorial/Lab 2 hour week
Resources to create online lab activities (met by CBA funding)

Text
The Art of Software Security Assessment

COMP6450 – Security Engineering Professional Practice

Justification
The professional practice of cyber security. Students learn how to be an effective cyber security professional.

Prerequisites
COMP3441

Coverage
Standards
Audits
Organisational Analysis and Testing
Best Practice
Ethics
Legal – Cybercrime, Censorship Terrorism, IP, Mandatory Disclosure, Privacy...
Institutional Response to Risk
Leadership
Change management
Professional Practice

Assessments
Fortnightly Case Studies
30% Portfolio
30% Presentation to external assessors (industry leaders)
10% Team Project
30% Final Written Exam.

Resource Implications
Lecture 2 hours/week – including guest lectures
Seminar 1 hour week
Resources to create online case studies (met by CBA funding)

COMP6448 – Security Engineering Masterclass

Justification
From time to time under our partnership arrangement with CBA we will have visiting experts coming to Sydney for one or two weeks. In that time we will use them to run intensive Masterclasses in their field of expertise for up to 24 students.

These courses could also be made available to paying students from industry.

Prerequisites
COMP6441 and Written application addressing the criteria appropriate for the particular masterclass.

Coverage
Vulnerability classes
Source code auditing
Fuzzing
Security Bugs
Software Security Assurance
Taint Analysis
Memory Corruption
Overflows
Return Oriented Programming

Assessments
Online exercises
Final Presentation
Portfolio

Resource Implications
Flying in an external expert (met my CBA funding)
LIC admin duties (1 hour/week)
Resources to create online lab activities (met by CBA funding)