Security Stream for Computer Science Degree

This offers a credentialed stream to undergraduate students intending to practice in Cyber Security in industry. This is a high demand area of employment and is forecast to have serious undersupply of graduates to at least 2025.

The cyber security education design is based on the security approaches of Ross Anderson and Bruce Schneier and incorporates an explicit engineering focus to security, rather than the more usual ah hoc “hacker”, or commercial “responsive” approaches of cyber security education.

The core courses in the stream teach analysis and systematic professional approaches to engineering security and examine failures, bugs, and human / system interactions and issues. There is an ongoing focus on security by design and professional ethical security practice.

Specialist elective courses allow students to specialise in their areas of interest and skill. Graduates of the stream are equipped for careers in penetration testing, Incident response, software assessment, malware analysis, forensics, military or law enforcement, security consulting, and security lead in dev teams.

This stream relies on students being exposed to C and to secure coding and vulnerabilities in first year including: memory use (data representation, the heap, function calls and the stack), and some assembly.

Note: we should consider moving from BSc (CompSci) to BCompSci (or similar) style naming so we can name the stream BCompSci (Security Engineering).

Compulsory

- COMP3441 Security Engineering; or
  COMP6442 Extended Security Engineering
- One of the starred electives below
- Two further electives drawn from the elective list (below)

Electives

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

  Secure web design and pen testing.
- COMP6445/6 – Digital Forensics/ Extended

  Forensics and Incident Response.
- COMP6447 – System and Software Security Assessment

  Content currently partially covered in 9447, 9447 coverage restored

  to original intent and matching name.
- COMP6450 – Security Engineering Professional Practice

  Cyber professional practice, law and ethics.
- COMP6448 – Security Engineering Masterclass

  Masterclasses led by visiting experts. Run as and 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 courses 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 but also covering the additional content topics, 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.

Handbook Entry

This is the extended version of COMP3441. This course includes the material of COMP3441 plus overage of reversing x86 machine code into C/C++ and an introduction to malware decomposition and analysis.

Student are assumed to have an understanding of C and memory organisation of modern computer systems. Student also need a keen devious and analytical mind.

CLO

COMP6443/4 – Web Application Security and Testing/ Extended

Justification

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: COMP3441/6442 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)

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 CPD.

Handbook Entry

6443:

Web applications are currently the predominant source of software vulnerabilities exploited in in online attacks. There is a growing need and growing demand for web programmers to be security aware.

This course covers the main types of web application vulnerabilities and current best practice professional coding and testing practices to be able to successfully develop secure web applications.

The course covers content and skills including 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. Course coverage will be constantly updated over time to reflect emerging vulnerabilities and practices.

6444:

This is the extended version of COMP6443. This course includes the material of COMP6443 plus penetration testing, and red teaming. Students will work in teams to conduct penetration tests and report on them to real and simulated clients.

COMP6445/6 – Digital Forensics/ Extended

Justification

Prerequisites

COMP3441/6442 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

+Extended Course: The Shell Coders Handbook

Handbook Entry

6445:

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

This course covers both forensic theory / professional practice, and looking at the underlying engineering of hiding, finding, interpreting and responding to traces. Students will use of standard forensic tools to extract carve and analyse data as well as learning the low level technical skills and knowledge underlying them. By the end of the course students should be able to write and analyse simple forensic tools as well as being able to use them.

The course covers Memory Forensics, Disc Forensics Network, Device Forensics, Stealth Techniques, Anti-forensics, Professional Forensic Practice, (chain of custody, records etc), Logging. Course coverage will be constantly updated over time to reflect emerging forensic practice and methods.

6446:

This is the extended version of COMP6445. This course includes the material of COMP6445 plus malware analysis and incident response.

COMP6447 – System and Software Security Assessment

Justification

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 by Mark Dowd, John McDonald, Justin Schuh

Network Attacks and Exploitation by Mathew Monte

Handbook Entry

6445:

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, analyse real world case studies of vulnerabilities in complex software used on widespread systems, and gain an understanding of the technical process of finding and fixing low-level software vulnerabilities and also of the economics and causal factors involved with their real world use.

The course covers techniques and skills including vulnerability classes, Source code auditing Fuzzing Security Bugs Software Security Assurance Taint Analysis Memory Corruption, Overflows, Return Oriented Programming Course coverage will be constantly updated over time to reflect emerging attack and defence methods.

6446:

This is the extended version of COMP6445. This course includes the material of COMP6445 plus malware analysis and incident response.

COMP6450 – Security Engineering Professional Practice

Justification

Prerequisites

COMP3441/6442

Coverage

Standards, Audits, Organisational Analysis and Testing, Best Practice, Ethics, Legal – Cybercrime, Censorship Terrorism, IP, Mandatory Disclosure, Privacy, Risk Assessment, 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)

The professional practice of cyber security. Students learn how to be effective and ethical cyber security professionals.

Delivery Notes:

In this course there will be regular guest lectures from senior industry practitioners and from experts in the course topics (e.g. law, ethical hacking, policy, regulation, law enforcement, national security, and leadership). Weekly case studies will be drawn from industry and student will be lightly mentored by industry practitioners and relevant experts (usually the guest speakers, or when senior, their junior staff) in the discussions and analysis of the fortnightly case studies.

Handbook Entry

6450:

The professional practice of cyber security. Students learn how to be effective and ethical cyber security professionals.

Students from this course will engage in real world case studies and analyse and critique effective professional responses to situations and challenges. Guest lecturers from Industry will give a number of different views into the world of cyber security professionals , the key issues they face, and current best practice.

The course covers Security Standards, Audits, Organisational Analysis and Testing, Best Practice, Ethics, Legal – Cybercrime, Censorship Terrorism, IP, Mandatory Disclosure, Privacy, Risk Assessment, Institutional Response to Risk, Leadership, Change management, and Professional Practice and professionalism.   Course coverage will be constantly updated over time to reflect emerging practices in the security engineering profession.

COMP6448 – Security Engineering Masterclass

Justification

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

Prerequisites

COMP3441/6442 and written application addressing the criteria appropriate for the particular masterclass.

Coverage

Advanced topics in Security Engineering – as able to be offered from visiting and local experts from time to time. It is envisioned that this course would only run when there are appropriate visiting experts. It could include advanced topics such as:

Ring 0 Rootkit detection, Advanced phone forensics, SCADA, Fibre Channel compromises, Advanced Exploitation techniques.

Assessments

Online exercises Final Presentation Portfolio

Resource Implications

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

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

Handbook Entry

6448:

This course is an intensive mode course on cyber security topics run at advanced level. It will run when we have an expert, such as a visiting expert, with a particular expertise. Advertised offerings will state the content being covered and the assumed knowledge and prerequisites for the course.

Admission is by LIC consent. Students are required to have passed 6447 or have equivalent evidence of capability; and apply to the LIC with a short statement explaining how they satisfy the prerequisites and assumed knowledge for the particular course being offered.