UNIVERSITY OF
OXFORD

software and systems security 2008/9

Welcome to *Software and Systems Security* at Oxford, a programme of advanced education for working professionals. The programme combines expert tuition in the fundamental principles, guidance in the application of the latest techniques, and an opportunity to learn more about the methods and tools that are essential to `best practice' in this important, emerging area of study.

Software and Systems Security

The security programme addresses security issues which arise throughout the systems life-cycle: from concept and inception, through design, implementation, testing, and deployment, to maintenance and re-engineering. This includes a detailed treatment of security risk and project risk, the social and organisational context, processes, patterns and architectures for security, and the technologies used in implementation and delivery.

The courses are delivered by an interdisciplinary team of subject specialists: lecturers and professors from the University of Oxford, working alongside colleagues from industry and the public sector to provide the necessary combination of academic rigour and practical experience. The security programme is part of a strong, long-established programme of professional education at Oxford, and participants can choose from a wide range of related courses in software and systems engineering.

"Never underestimate the time, expense, and effort an opponent will expend to break a code."
(Robert Morris)

Qualifications

Students on the programme can work towards one of three postgraduate qualifications from the University of Oxford: the Postgraduate Certificate, the Postgraduate Diploma, and the MSc in Software and Systems Security. They can choose also to take one or more of the courses as part of an informal programme of study, or as part of Oxford's MSc in Software Engineering.

Mode of study

Each course includes an intensive teaching week of classes, lectures, and practical work, followed by a written assignment. Students working towards a qualification typically take three or four of these courses a year. Courses take place at the programme's purpose-built facilities in the centre of Oxford, and class sizes are kept small to allow for a high degree of interaction. This mode of study is particularly effective for those with professional or personal commitments.

Who should apply?

The programme assumes an understanding of the importance of security, and an awareness of security issues, such as might be expected in a professional whose role or ambition includes the design, development, management, or application of information systems. Existing students include software developers, technical leads, programme managers, and independent consultants.

There are no formal entry requirements for the individual courses, although prospective attendees are asked to confirm that satisfy the basic requirements, in terms of experience and relevant education, for any courses that they wish to attend. For the postgraduate qualifications, applicants are expected to have an undergraduate degree in a relevant discipline and/or an appropriate amount of professional experience.

Postgraduate qualifications

All of the courses offered by the programme are taught at Master's level: the three postgraduate qualifications differ only in the extent of study.

Postgraduate Certificate

This qualification requires attendance on courses in four subjects, and the successful completion of the corresponding written assignments. At least three of these subjects must be chosen from the courses in software and systems security; subjects in software engineering are also available for the fourth choice. The courses and assignments must be completed within two years of the date of admission.

Postgraduate Diploma

This qualification requires courses in eight subjects. At least six of these subjects must be chosen from the courses in software and systems security; the remaining two subjects may also be chosen from subjects in software engineering at Oxford. The courses and assignments must be completed within three years of admission.

Master of Science

This qualification requires courses in ten subjects; it also entails the completion of a project and dissertation, involving participation in a project module and a dissertation module. At least seven of these subjects should be chosen from the core selection of courses in software and systems security; others may be chosen from across the whole range of subjects offered in software engineering at Oxford. The courses and assignments should be completed within four years of admission; an additional year is available, if needed, in which to complete the dissertation.

Admission

Applications for part-time, postgraduate study are invited from anyone with sufficient experience or proven ability in the field of software engineering or security.

A typical applicant might have an undergraduate degree in a related subject, and at least two years' experience of software or security development in an industrial context. However, relevant experience may compensate for a lack of formal qualifications, or vice versa — candidates should contact the Programme Office for further information.

The open nature of the entry requirements means that a formal interview is an essential part of the admissions process. Prior to the interview, applicants are asked to present two references from people who are familiar with their work or study achievements and — if appropriate — to secure the support of their employer.

Successful applicants will become registered students of the University with effect from the beginning of the next University term. New students who have already attended courses on the programme can use those courses as credit towards their qualification, provided that the course dates are within one year of the date of admission.

Previous study

A student on the programme may be able to use a course taken elsewhere as credit, provided that: the course was taught and assessed at the same level; the subject fits within the programme curriculum; and the course is not used as credit towards any other qualification. For the Postgraduate Certificate, no more than one course taken elsewhere may be used; for the Postgraduate Diploma or the MSc, no more than two.

Research activity

The programme is also a centre for research activity. The teaching staff are involved in a number of national and international projects in the areas of: large-scale data integration and sharing, particularly regarding authorization; cancer clinical trials informatics; applications of trusted infrastructure technologies in distributed systems; and secure system design, particularly issues surrounding the usability of secure systems.

Software and Systems Security Courses

As computing systems become more essential to our daily lives, it becomes ever more important that the services they provide are available whenever we need them. We must also be able to rely on the integrity of the systems, and thus the information that they hold and provide. What is more, our society and our economy depend upon certain pieces of information being held in confidence.

Security Principles (SPR)

This course combines a treatment of the fundamental principles of cryptography and security protocols with a practical treatment of current best practice. It explains the need for computer security, and the scope of the available technical solutions; presents techniques for evaluating security solutions; and provides an overview of the current leading technologies and standards in the security arena.

"Security is not a product; it itself is a process." (Bruce Schneier)

Design for Security (DES)

Capability in the design of systems which will meet security goals is an increasingly important skill. This course explores how cost-effective solutions to security needs can be achieved by following well-established architectural practices and detailed security principles. Central to these considerations is the need for requirements to be met with established solutions, and how a balance can be struck between security and other system requirements.

Participants should have a basic understanding of topics in security, as provided by the *Security Principles (SPR)* course.

Security Risk Analysis and Management (RIS)

Security is a property of an entire system in context, rather than of a software product, so a thorough understanding of system security risk analysis is necessary for a successful project. This course introduces the basic concepts and techniques of security risk analysis, and explains how to manage security risks through the project lifecycle.

Participants should have a basic understanding of topics in security, as provided by the *Security Principles (SPR)* course.

RIS

SCS

DES

PAS

SPR

SRO

FOR

TCI

NES

Bodleian Library, University of Oxford

People and Security (PAS)

A very high proportion of failures in security can be attributed to human weakness, misunderstanding, mis-information, or failure to grasp the importance of the processes individuals are expected to follow. This course draws on work from human-computer interaction, and more widely from psychology, relating these issues back to hard technical implementation decisions.

Familiarity with basic security principles and standard mechanisms, as covered in *Security Principles (SPR)*, is assumed.

Secure and Robust Programming (SRO)

Many system failures and security vulnerabilities arise at the programming level. These can often be attributed to inadequate handling of exceptional situations, poor understanding of the details of the programming language in use, incomplete descriptions of the interfaces between components, and insufficient care in the treatment of concurrency and threading issues. This course addresses those problems from a programming perspective, with the aim of improving the practitioner's capability in writing and reviewing code.

Participants should have a basic understanding of topics in security, as provided by the *Security Principles (SPR)* course.

Forensics (FOR)

Investigating computer crime is a delicate and involved process that requires an understanding of the evidential standards necessary in various contexts where electronic forensic data may be needed. This course describes the current best practice in both understanding and deconstructing an attack whilst preserving evidence, and also explores how to design and evaluate systems in order to facilitate forensic examination.

Participants should have a basic understanding of topics in security, as provided by the *Security Principles (SPR)* course.

"Being able to break security doesn't make you a hacker anymore than being able to hotwire cars makes you an automotive engineer."
(Eric Raymond)

Network Security (NES)

Modern computing systems— whether PCs, PDAs, mobile phones, or other application-specific devices— are nearly all networked. These networks are far from homogeneous, but all give rise to substantial challenges for security. This course concentrates on devices with internet connections, reviewing the internet design features, and their consequences for security.

Participants should have a basic understanding of topics in security, as provided by the *Security Principles (SPR)* course.

Trusted Computing Infrastructure (TCI)

A secure system is the product of numerous layers that operate together to provide in-depth protection. This course looks at the various platforms upon which a secure system operates, with an emphasis on practical and repeatable means of implementing these platforms securely. Topics covered include buffer overflows, cryptographic libraries, sand-boxing, virtualisation, trusted computing, and database security, building towards a toolkit of sound principles for secure systems implementation.

Participants should have a basic understanding of topics in security, as provided by the *Security Principles (SPR)* course.

Safety Critical Systems (SCS)

Computers are often placed in control situations within safety-critical systems. Safety is an emergent property of whole systems; software may play only a small part. This course will enable the systems engineer to determine whether a safe system can be built, and what requirements must be placed on software in order to keep risk at an acceptable level. Attendees will be able to understand the specific issues, problems and techniques associated with analysis, design, development and verification of systems that will be used in safety critical applications.

Bodleian Library, University of Oxford

Software Engineering Programme

The Software Engineering Programme is the result of a collaboration, established in 1992, between Oxford University Computing Laboratory (OUCL) and Oxford University Department for Continuing Education (OUDCE). OUCL has an international reputation for linking mathematical theory to industrial practice. OUDCE has a distinguished history in promoting life-long learning, including delivering high-quality education to working professionals.

There are three themes to the software engineering courses: Modelling, Architecture, and Process. Each of these covers different aspects of software engineering, and there are currently seven courses in each theme.

The security programme is fully integrated with the Software Engineering Programme, allowing students on either programme of study to attend courses from both portfolios. The following are a selection of courses in software engineering that may be of interest to students studying Software and Systems Security. See *www.softeng.ox.ac.uk* for the full list.

Software Engineering Mathematics (SEM)

An important characteristic of a specification is the ability to reason about the objects it describes, and thus about the system it models. If that specification is written mathematically, the reasoning can take the form of calculation: we can use simple, logical methods — and tool support — to check that a specification is consistent, and to predict the consequences of our design decisions. This course is an introduction to mathematical description, using basic set theory and logic.

Concurrency and Distributed Systems (CDS)

The consequences of design decisions are particularly hard to predict when a system consists of several concurrently-executing components, or when there is a complex pattern of interaction between a system and its environment. This course presents a powerful technique for describing the intended behaviour of concurrent systems, and for reasoning about the patterns of interaction that may emerge.

Service-Oriented Architecture (SOA)

The current consensus on best practice for building component-based distributed applications is to use a *service-oriented architecture*. Services are encapsulated behind carefully-designed simple interfaces, and the realities of heterogeneity, decentralization and fault tolerance are embraced rather than ignored. The course provides an understanding of the strengths and weaknesses of service orientation, informed by an ability to implement and deploy simple web services using a suitable development platform.

Mobile and Sensor Networks (MOB)

Recent advances in wireless mobile and sensor technologies have changed computing, enabling application scenarios in which large numbers of pervasive computing devices are connected to a wireless networking infrastructure in an ad hoc manner. This course covers communication protocols for mobile ad hoc networks, and provides an overview of distributed data management techniques for resource-constrained sensor networks.

Management of Risk and Quality (MRQ)

Too many project planning approaches concentrate on just the estimating and network aspects of planning. This is of little value if the project is given the wrong shape or the wrong activities are chosen in the first place. The *Strada method* taught in this course builds the project from an analysis of the specific risks to be faced. It then uses an analysis of the specific quality requirements to fill out the detail. The two perspectives of risk and quality prove sufficient to give the basis for a reliable and robust plan.

Process Quality and Improvement (PRO)

Every software development organization needs to be focused on the delivery of quality. The software engineering discipline responds by calling for a managed process for the construction and testing of software, and for the improvement of that process. This course explains the necessary concepts within the frameworks provided by three important international standards.

Examination

A student who has completed the required number of courses and written assignments may enter for examination as soon as the minimum period of study has elapsed: for a Postgraduate Certificate or Postgraduate Diploma, this means one year after first admission; for the MSc, at least two years after first admission, and at least one year after transferring registration to the MSc.

Each written assignment is treated as part of an examination at the University of Oxford. Assignment submissions and assessment reports are reviewed by a board of examiners — all subject specialists — before a grade is assigned, and a copy is returned to the student.

When a student enters the examination for a postgraduate qualification, the examiners consider their performance at the next formal meeting; there is a meeting at the end of each University term. They may also wish to interview the student, to ask about the work that they have submitted and the courses that they have attended. Should a student fail to satisfy the examiners, they would be given an additional year in which to undertake further study.

Kellogg College

A student requesting a change to MSc registration will be required to complete a college application form. If the request is appropriate, it will be forwarded to the University's Graduate Studies Office, who will deal with the college in question. If the application is approved, then the student will be required to matriculate, normally during the next University term. The student then becomes a member of their chosen college.

There are many different colleges, each with its own style and tradition, and one of them is closely associated with part-time study. It was named in honour of William Keith Kellogg, industrialist and philanthropist, in recognition of the support given to adult and continuing education by the W. K. Kellogg Foundation.

Kellogg has approximately ninety fellows (including all of the Programme's University Lecturers) and approximately four hundred registered students. Most of the Programme's students who progress to the MSc apply to Kellogg. The College organises regular events, and acts as an additional point of contact between MSc students and the University.

Fees

There is a standard fee of £1400 for each course attended, payable in advance. This includes course materials, and lunches during the teaching week, but not accommodation. The fee applies whether or not the attendee is working towards a postgraduate qualification, and regardless of nationality and residency. The Postgraduate Certificate will typically entail four course attendance fees, the Postgraduate Diploma eight, and the MSc ten. The MSc also requires attendance at a week-long project module in Oxford, and passing a dissertation module. There is no course fee for either of these modules — the cost is included in the student registration fee for the MSc.

Students may cancel attendance, provided that the cancellation is received well enough in advance. Cancellations at short notice may not receive a full refund of the course attendance fee.

The examination and assessment of the course assignment is included in the course attendance fee. Should a student be granted permission to take the assignment for a later course in the same subject, an additional examination fee of £100 will apply.

There is an annual student registration fee of £2520 for any of the postgraduate qualifications; this is payable for one year for a Postgraduate Certificate, two years for a Postgraduate Diploma, and four years for an MSc. Students who are citizens of a member state of the European Community, and have been ordinarily resident in the European Economic Area for the past three years, may qualify for Home/EU status, and a reduction of this annual award fee to £1490.

All payments must be completed before any postgraduate qualification will be awarded by the University. Award fees are based upon the date of admission. Attendance fees are based upon the date of the course, and may increase during the period of study, typically in line with the rate of inflation in the UK.

Taking part

To reserve a place on a course *without* first becoming a registered student, you should complete the course booking form. If a place is available, you will receive a confirmation from the Programme Office. For courses in certain subjects — *DES*, *FOR*, *NES*, *PAS*, *RIS*, *SRO*, and *TCI* — you may be asked to confirm that you have sufficient experience before your reservation can be approved.

Students who *are* registered for a postgraduate qualification do not need to submit booking forms for individual courses: they can make reservation requests via the Programme website.

Postgraduate study

To apply to study for a postgraduate qualification, you should follow the procedure on the Programme website, or request an information pack from the Programme Office. Either route provides instructions on what supporting documentation you should supply.

Only those applicants with an appropriate combination of education and experience will be called to interview. Applicants should not make travel plans, or accept contingent financial (or other) commitments, unless a formal, written offer of a place has been made. The allocation of a place on an *individual course* does not imply admission to a postgraduate qualification.

Contact

Enquiries should be addressed to the Programme Office:

    Software Engineering Programme
    Wolfson Building, Parks Road
    Oxford OX1 3QD, UK
    +44 1865 283525 (phone), 283531 (fax)

The most effective means of contact is email:
    info@softeng.ox.ac.uk

Further information about the Programme, together with course booking and application forms, can be found on the Programme website:
    www.softeng.ox.ac.uk/security