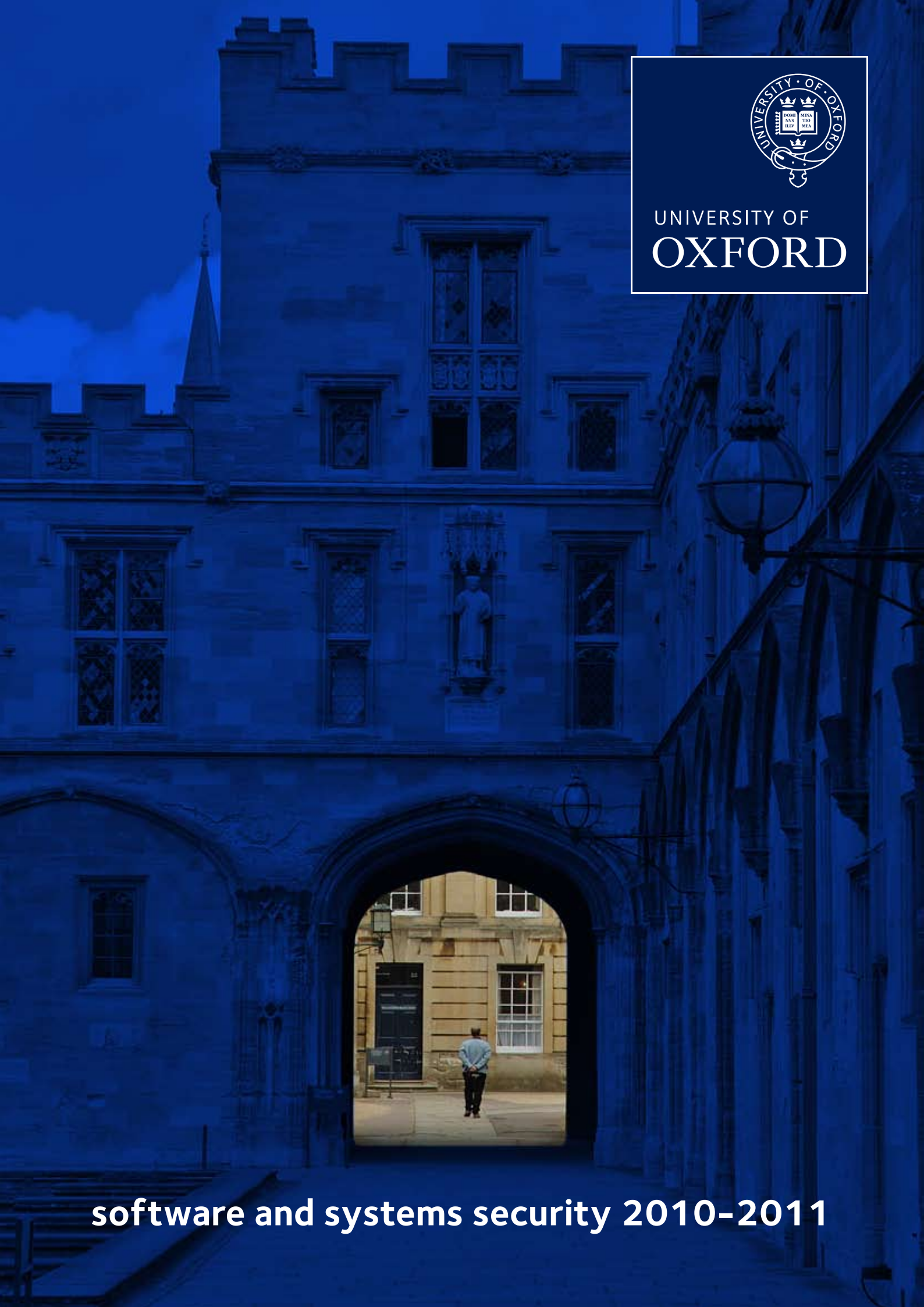


software and systems security 2010-2011

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 usually work towards an MSc in Software and Systems Security from the University of Oxford. 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 MSc, applicants are expected to have an undergraduate degree in a relevant discipline and/or an appropriate amount of professional experience.

Master of Science

All of the courses offered by the Programme are taught at the Master's level. The MSc in Software and Systems Security 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 six of the taught subjects, and the dissertation, 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 — 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.

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

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. The third theme of courses on the Programme concerns software and systems security, from both social and technical points of view.

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

Security Principles

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. It also provides an introduction to the whole Software and Systems Security theme.

Design for Security

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 meeting requirements with established solutions, and striking a balance between security and other system requirements.

Security Risk Analysis and Management

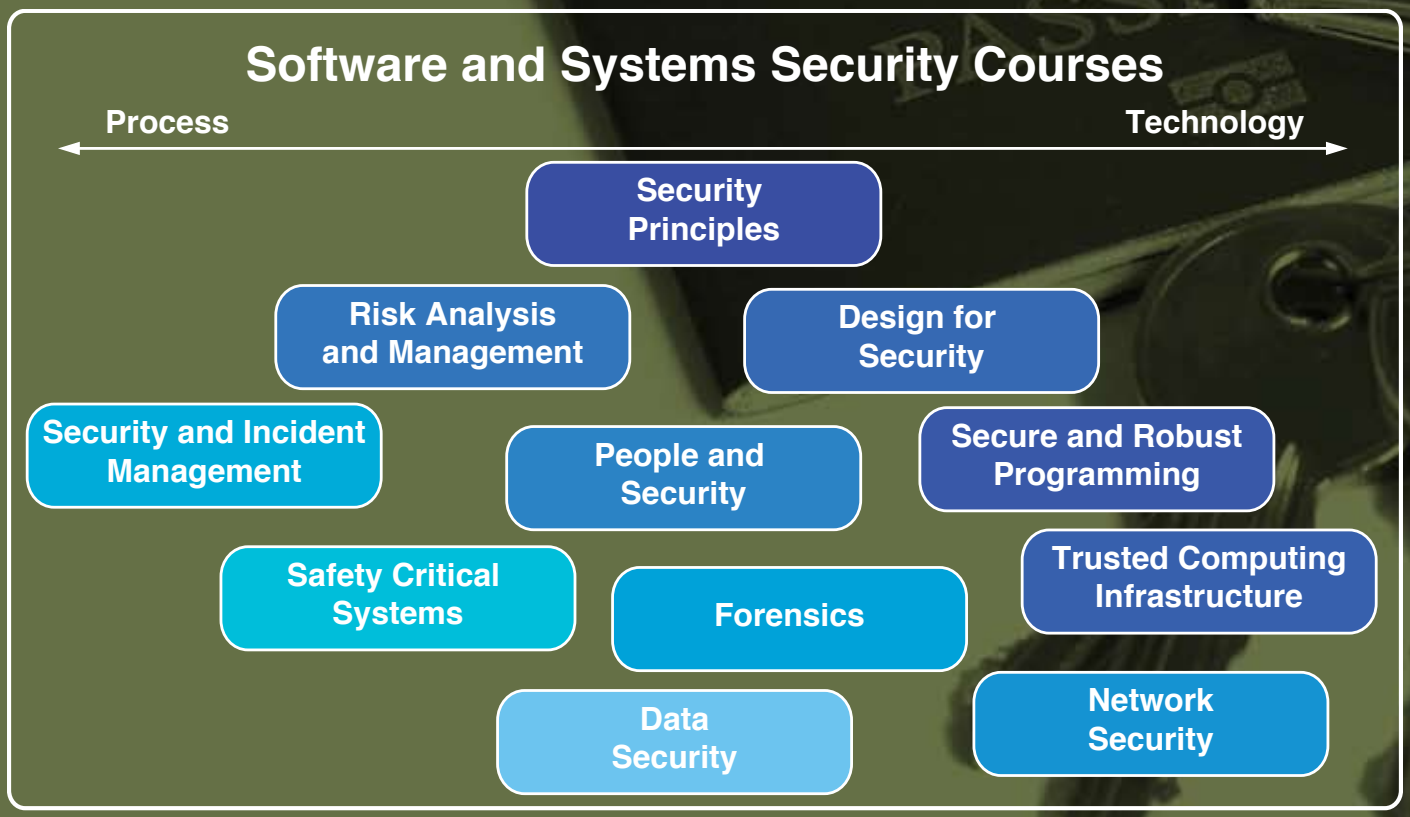
Security is a property of an entire system in context, rather than of a software product, so a thorough understanding of system security risk analysis is necessary for a successful project. This course introduces the basic concepts and techniques of security risk analysis, and explains how to manage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

Security and Incident Management

A key ingredient of successful security and risk programmes is effective management of security-related incidents. Incidents range from small and predictable — which can be eliminated through operation controls, through to large and unpredictable — when standard management controls and mechanisms may not work. This module introduces the principles of incident management in practical contexts and draws out the key themes for effective response to the panoply of events and triggers that impact businesses, governments and individuals alike.

People and Security

A very high proportion of failures in security can be attributed to human weakness, misunderstanding, misinformation, 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.




Bodleian Library, University of Oxford

Secure and Robust Programming

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, and incomplete descriptions of the interfaces between components. This course addresses those problems from a programming perspective, with the aim of improving the practitioner's capability in writing and reviewing code. Topics include animation of specifications, static analysis, design by contract, run-time assertion checking, and compile-time verification.

"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)

Safety Critical Systems

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.

Data Security

As increasing amounts of data are captured about patients, consumers and citizens, and as more ways of linking and utilising such data emerge, so do concerns about the treatment of personal data — with these concerns emerging from a variety of stake-holders. As such, issues pertaining to database and applications security have increased in importance in recent years. Understanding how existing and emerging legislation might be considered in designing secure databases, as well as how such designs might be mapped to practical security measures, will be essential in an increasingly data-driven world.

Forensics

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.

Trusted Computing Infrastructure

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.

Network Security

Networking technologies play a critical role in almost all modern software-based systems, whether the fixed networks of computers we now regard as commonplace, or the growing cloud of pervasive devices which have increasingly diverse profiles of network connectivity. As a result, networks provide a potential vector for many forms of attack, and are an ideal location for many threat mitigations and isolation technologies. Much benefit has been derived from a layered approach to network architecture, and most approaches to security are aligned to those boundaries. This course will consider the prevention, detection, mitigation, and remediation of security problems in the network at each level of abstraction, as well as looking at cross-cutting concerns across the whole stack.


Bodleian Library, University of Oxford

Software Engineering Programme

The MSc Programme has been run by Oxford University Computing Laboratory (OUCL) for over fifteen years. OUCL is one of the world's leading computer science departments, with an international reputation for excellence in both pure and applied research, and a strong focus on software and systems security.

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 is 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

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

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.

Object-Oriented Programming

This course teaches the concepts and principles of object-oriented programming. The language used is Java, although most of the material covered will apply equally well to any other object-oriented language: objects, methods, interfaces, messages, and events.

Process Quality and Improvement

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.

Management of Risk and Quality

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.

Service-Oriented Architecture

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.

Examination

"All of the Programme's examinations are in the form of take-home assignments: there are no short, closed, examinations in the traditional style. 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 (two years after first admission) has elapsed.

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, 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.

Oxford Colleges

Every MSc student has to join a college and attend a matriculation ceremony. 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 College has approximately ninety fellows (including all of the Programme's University Lecturers) and approximately four hundred registered students. Most of the Programme's students apply to Kellogg. The college organises regular events, and acts as an additional point of contact between MSc students and the University.

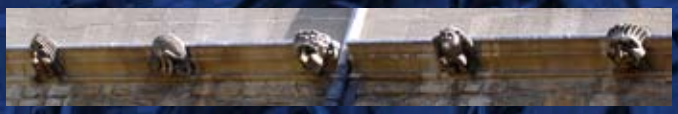
Taking part

To reserve a place on a course, you need first to be registered with the Programme (just click on *Sign in or Register* on the front page of the website). If a place is available, you will receive a confirmation from the Programme Office. For courses in certain subjects, you may be asked to confirm that you have sufficient experience before your reservation can be approved.

Postgraduate study

To apply to study for an MSc, 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 and until 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.



Fees

There is a standard fee of £1500 for each course attended, payable in advance. This includes course materials, and lunches during the teaching week, but not accommodation. The course fee applies whether or not the attendee is working towards an MSc, and regardless of nationality and residency. The MSC will typically entail ten course attendance fees. It 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 £2650 for the MSc, payable for four years. 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 £1625. Thus the current cost of an MSc, assuming the expected minimum number of course attendances, is £21500 at the home rate and £25600 at the overseas rate.

All payments must be completed before any postgraduate qualification will be awarded by the University. Fees will increase annually, broadly in line with the rate of inflation in the UK.

Contact

For enquiries, contact 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