MSc in

Software and Systems Security

flexible, part-time, professional education

UNIVERSITY OF OXFORD

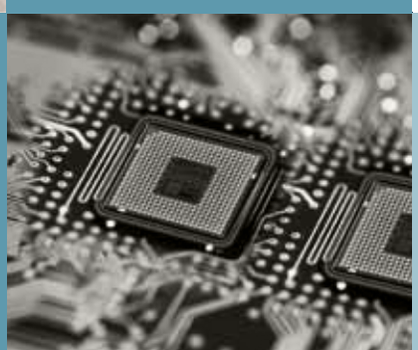
Software and Systems Security

As computing technologies become more pervasive, more connected, and more indispensable, the security of the systems they support becomes more important. We rely on these systems for the success of business and other ventures, for the safety of family and friends, and for our personal convenience. We want to be assured that they will work exactly as expected, and that they will keep working – even in the face of disasters, accidents, or deliberate attempts to interfere with or prevent their function.

Achieving and maintaining security is a complex, interdisciplinary challenge. We must consider not only the software and hardware components of a system, but also the way in which these relate to the human processes and physical constraints of the real world. A modern security professional needs to understand principles of architecture, design, management, interoperability and evolution, and to apply them effectively in a world of rapidly-changing technologies and expectations.

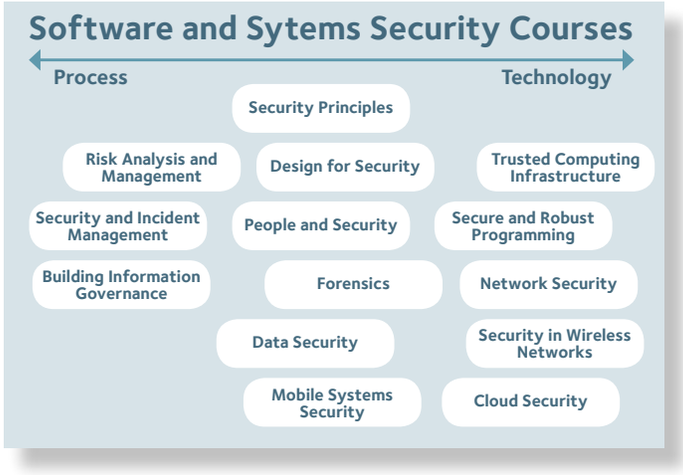
The Software and Systems Security Programme at the University of Oxford teaches these principles and their application. It offers a flexible programme of short courses to those working full time in industry or in the public sector. It addresses a wide range of subjects – from service architectures to forensics, from trusted platforms to risk analysis, and from human factors to incident management. It is accessible to anyone with the right combination of previous education and practical experience.

The courses on the Programme can be used as individual programmes of professional training in specific subjects, or as credit towards a Master of Science (MSc) degree in Software and Systems Security from the University of Oxford. Students on the MSc take between two and four years to complete a minimum of ten courses, typically at a rate of three courses per year, earning a degree while in full time professional employment. The courses may be taken in any order and combination, depending upon previous experience and education.



Courses in Security

Each short course is based around a week of intensive teaching in Oxford, with some initial reading to consider beforehand, and a six-week assignment to complete afterwards. The teaching week allows you the chance to explore a subject in depth, with expert teaching and supervision, away from the demands of work and family. The reading gives you the opportunity to prepare yourselves; the assignment, an opportunity to deepen and to demonstrate your understanding.



Security Principles SPR

This course teaches the fundamental principles of information and systems security, and is often used as an introduction to the Programme. It explores a wide range of security technologies, examines security standards and expectations, and explains techniques for the evaluation of security requirements and solutions. It places theoretical work on protocol design, cryptography, and information flow firmly in the context of existing and emerging practice, with an emphasis upon integration and usability.

Design for Security DES

Security is a system-level property, and emerges from the coordinated design of components and processes. This course shows how a range of factors, from architectural patterns to detailed technical controls, can be considered together in the production of cost-effective solutions. It addresses the challenge of providing security, through a combination of infrastructure, mechanisms, and procedures, while satisfying requirements for functionality and usability.

Security Risk Analysis and Management RIS

The concept of risk is central to software and systems security. An understanding of the ways in which systems are exposed to different kinds of threat, and an appropriate assessment of likelihood and impact, can inform the selection and prioritisation of security measures. This course teaches a principled approach to risk analysis, explores the techniques and practices of risk management, and demonstrates their application through a realistic set of examples and case studies.

People and Security PAS

Many failures in security can be attributed to human weakness, misunderstanding, misinformation, misdirection, or failure to grasp the importance of prescribed processes and procedures. The interaction between people and technology often presents a significant challenge to secure operation. This course teaches techniques drawn from human-computer interaction and psychology, addressing this challenge within the context of hard, technical implementation decisions.

Forensics FOR

The investigation of computer crime is a delicate, involved process that requires a deep understanding of the evidential standards expected in circumstances where electronic forensic data is to be used. This course describes the current best practice in understanding and deconstructing an attack whilst preserving evidence, and explores how to design and evaluate systems in order to facilitate forensic examination. It combines a strong overview of principles with some illustrative practical work, recovering data using necessarily low-level tools.

Network Security NES

Networks are a potential vector for many forms of attack, and are an ideal location for threat mitigation and isolation technologies. This course teaches approaches to the prevention, detection, mitigation, and remediation of security problems in the network at each layer, as well as looking at cross-cutting concerns across a complete networking stack. It examines the strengths and weaknesses of boundary protections, intrusion detection and prevention, and privacy-preserving routing.



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. It examines roots and chains of trust, operating systems security, trusted platforms, and virtualisation for security. It shows how these are applied to secure networking, remote working, trusted storage, and remote computation in grids and clouds.

Mobile Systems Security MSS

Mobile devices present distinctive challenges for security, including problems of device association, power constraints, and restricted interfaces. Mobile applications often incorporate both local and remote services, complicating the management and enforcement of security policies. This course presents a range of techniques for the design and implementation of secure mobile applications, balancing the requirements of functionality, security, resource utilisation, and privacy.

Security Incident Management SIM

A key ingredient of successful security and risk programmes is effective management of security-related incidents. Incidents range from the small and predictable, which can be eliminated through operation controls, to the large and unpredictable, where standard management controls and mechanisms may not work. This course teaches the principles of incident management in practice and identifies key themes for effective response to the range of events and triggers that impact upon businesses, governments, and individuals.

Secure and Robust Programming SRO

Many failures and vulnerabilities arise at the programming level. These are often due 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 aims to improve the practitioner's capability in writing and reviewing code, through a thorough understanding of static analysis, run-time assertion checking, and compile-time verification.

Security in Wireless Networks SWN

Wireless and mobile networks are familiar from everyday life, but present a distinctive mix of security challenges, as a result of trade-offs between power, cost, physical propagation characteristics, interfaces, modes of use, and management. Moreover, as they often are associated with the individual,they are often of central importance in concerns of privacy. The purpose of this course is to familiarise participants with threats, vulnerabilities,and security countermeasures of core technologies such as WLAN, Bluetooth, GSM, and UMTS, as well as new and emerging wireless technologies, such as ZigBee, wireless mesh networks, and RFIDs.

Cloud Security CLS

The provision of automated self-managed services – for software, platforms, and infrastructure – relieves local administration of many security concerns, yet also removes from them many of the tools and controls they expect to use, while introducing new threats and adversaries. This course reviews the architectural principles of cloud computing, describes the threats and security controls possible at each level of abstraction, and addresses cloud management services for trustworthy, secure, and resilient operation with minimal intervention.

Data Security and Privacy DAS

New technologies make it possible to capture increasingly detailed, personal information: about customers, patients, and citizens. As new ways of linking and using this information emerge, so too do concerns about the security of the corresponding data. This course explores the potential impact of existing and future legislation upon data storage and processing, and presents practical approaches to the secure management of personal and other information in databases and applications.

Building Information Governance BIG

To govern information now requires mastery of a diverse, often international, portfolio of legal rules, technology standards, business policies and technology, all applied across increasingly complex, distributed systems and repositories. The increase scrutiny and requirements of official agencies and business partners impose new requirements for compliance documentation and transparency. This course introduces a structured design approach that enables strong, responsive, and resilient information governance to be incorporated into the design and management of digital assets.

Courses in Software Engineering

A range of other courses are available, addressing subjects in software engineering. These may address complementary topics, or provide useful background, for the study of software and systems security.

Software Engineering Methods

These courses assume an understanding of the issues and challenges of software development.

Requirements Engineering (REN) introduces techniques for requirements elicitation and analysis in the context of software design and development.

Agile Methods (AGM) shows how to select, apply, and evaluate agile methodologies, and how to manage the relationship between the customer and the development team.

Management of Risk and Quality (MRQ) teaches well-founded and practical techniques for risk analysis and quality assurance in software project management.

Process Quality and Improvement (PRO) explains how to evaluate development activities against standard models, and how to define quality frameworks for delivery.

Safety Critical Systems (SCS) explores a range of methods and tools for the development of software for safety critical applications.

Software Development Management (SDM) teaches the techniques of development management, and develops the skills needed to manage innovative technologies.

Interaction Design (IDE) introduces the factors, techniques, tools, and theories that can help in designing usable systems.

Software Engineering Mathematics (SEM) shows how to use basic logic and set theory to describe, reason about, and understand properties of software and systems.

Specification and Design (SDE) explains how to create precise models of structure and functionality, and how to check the consistency of sequential descriptions.

Concurrency and Distributed Systems (CDS) presents a modelling language, and supporting tools, for the description and analysis of concurrent behaviour.

Model Checking (MCH) explores the application of model-checking techniques to the analysis and verification of large, complex systems.

Performance Modelling (PMO) teaches analytical methods and tools for improving the efficiency and productivity of computing and communications systems.

Enterprise Architecture (EAR) explores how to create and manage very large information infrastructures, consisting of hundreds or thousands of systems, and contrasts this with the approaches to architecture needed when designing a single system.





Software Engineering Tools

These courses assume a familiarity with modern programming languages, tools, and techniques.

Service Oriented Architecture (SOA) explains how to design applications as compositions of services, and how to reliably determine the properties of these compositions.

Mobile and Sensor Networks (MOB) presents communication protocols and management techniques for wireless, mobile, and ad hoc networking.

Database Design (DAT) teaches the principles of relational database design, from schemas and constraints to concurrency and distribution.

Software Testing (STE) explores methods and tools for the derivation and application of tests from specifications, design artifacts, and source code.

Object Orientation (OOR) offers an introduction to the subject for novices, but also a wider perspective for experienced users.

Object Oriented Design (OOD) teaches standard techniques for the specification and design of software systems, using the Unified Modeling Language and related notations.

Object Oriented Programming (OOP) presents the principles of object-oriented programming, from encapsulation to identity, and shows how to apply them in any language.

eXtensible Markup Language (XML) explores the use of markup and meta-languages for data description and transformation.

Functional Programming (FPR) provides new perspectives on algorithm design, data structures, and functional abstraction.

Concurrent Programming (CPR) explains how to implement concurrent, scalable, real-time systems, with an emphasis upon fault tolerance and high availability.

Design Patterns (DPA) shows how to use a language of patterns to find and to record solutions to recurring problems of system architecture.

Agile Practices in Engineering (APE) provides an understanding of and practical experience in techniques for building software in an agile environment.

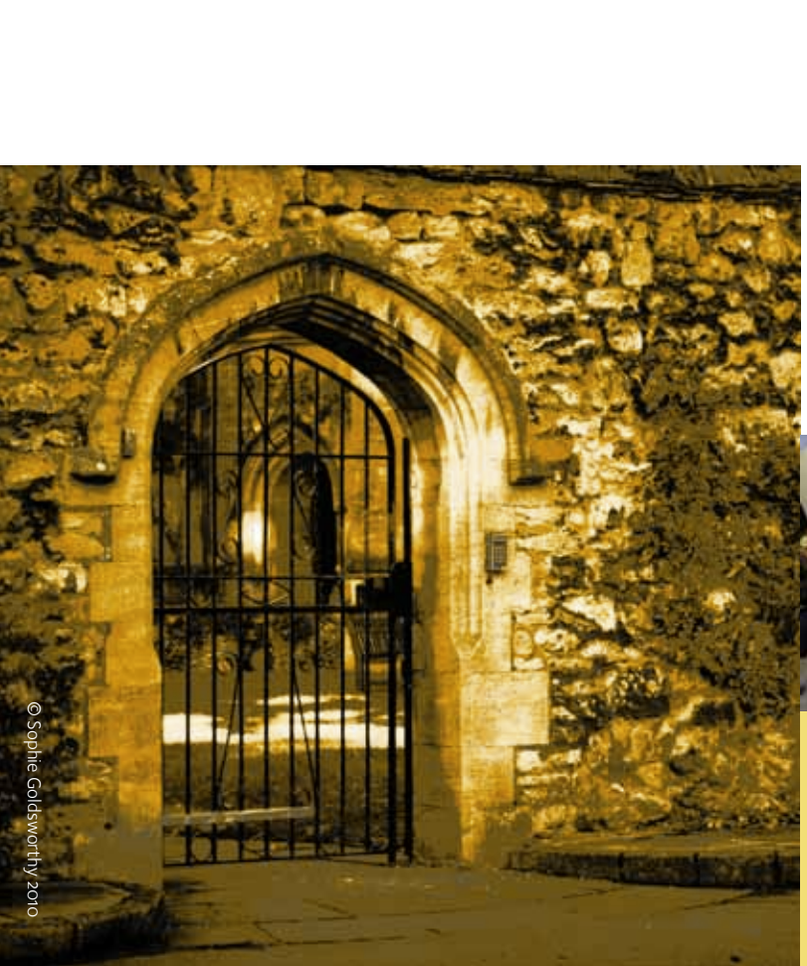
Software Product Lines (SPL) presents methods and tools for software re-use, aspect- and feature-oriented design, and product customisation.

"The MSc looks impressive on a resume. It has certainly opened a number of doors for me"

MSc in Software and Systems Security

A postgraduate degree is evidence of individual ability and understanding beyond the expectations of industry training, undergraduate education, and professional experience. It is a demonstration that you have achieved a mastery of the subject: that you can select, adapt, and apply appropriate techniques; that you can evaluate what is, and what is not, working; that you can anticipate, and facilitate, change. This kind of evidence can be invaluable in the workplace: to lend additional authority to your opinions; to better establish your credentials; and to reassure others as to your suitability for new roles and responsibilities.

A postgraduate degree is also an opportunity for personal development: a chance to test your ideas and intuitions, to experiment with new tools and techniques, and to make new connections between theory and practice. It is an environment in which you can take a step back from the immediate demands and compromises of your latest project, and think more strategically about the nature of the problems you encounter, and how they might be solved more efficiently and more effectively. This kind of opportunity can be invaluable in your personal life, bringing new confidence, skills, and inspiration.



The University of Oxford

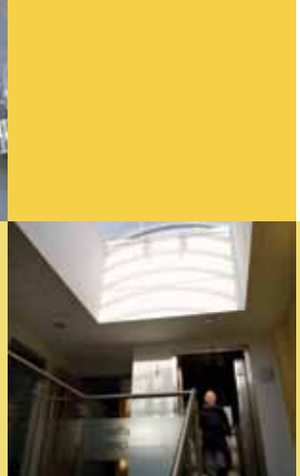
The courses take place in a purpose-built teaching facility in Oxford, in the Department of Computer Science. Each course is taught by a subject expert: a member of faculty, or an industrial practitioner. The students will bring a varying combination of expertise and experience: some will be security specialists, managers, or consultants; others will be architects, designers, or developers addressing security issues and concerns. Class sizes are kept small to facilitate learning and interaction.

All students are members of the University's Department of Computer Science, a recognised centre of excellence for teaching and research in computing and related disciplines. The University of Oxford was the first university in the English-speaking world, and is consistently ranked among the ten leading universities globally.

Each student will be a member also of one of the Oxford colleges. Several colleges offer places for this course, but most students choose to belong to Kellogg College, a college established specifically to meet the expectations of students on professional and non-residential programmes. If a student on the programme already has a degree from Oxford, and was a member of a different college for their previous period of study, then they may prefer to return to that college. All of the faculty whose teaching is primarily of part-time students are themselves members of Kellogg.

UNIVERSITY OF OXFORD

DEPARTMENT OF COMPUTER SCIENCE



Studying on the Programme

Getting Started

All of the courses described above can be taken as individual programmes of professional training. You may book a place on any course on-line, or by calling the Programme Office. One month before the teaching week – or upon payment of the invoice, if later – you will be sent some initial reading material. The teaching week itself runs from 9 a.m. to 5 p.m. from Monday to Thursday, and from 9 a.m. to 12.30 p.m. on Friday. At the end of the week, you will be given an assignment task: you can take this, and get feedback on your submission, even if you have no plans to use the course as credit towards a postgraduate qualification.

To study for the MSc in Software and Systems Security you need to make a formal application to the University. You can take up to two courses before doing this and still use them as credit, provided that you complete the assignments. If you appear to meet the admission criteria, you will then be invited for an interview, where you will have the opportunity to discuss your expectations, your study plans, and your readiness to take part in a programme of part-time, professional education. If your application is successful, then you may be admitted at the beginning of the next term: in January, April, or October.

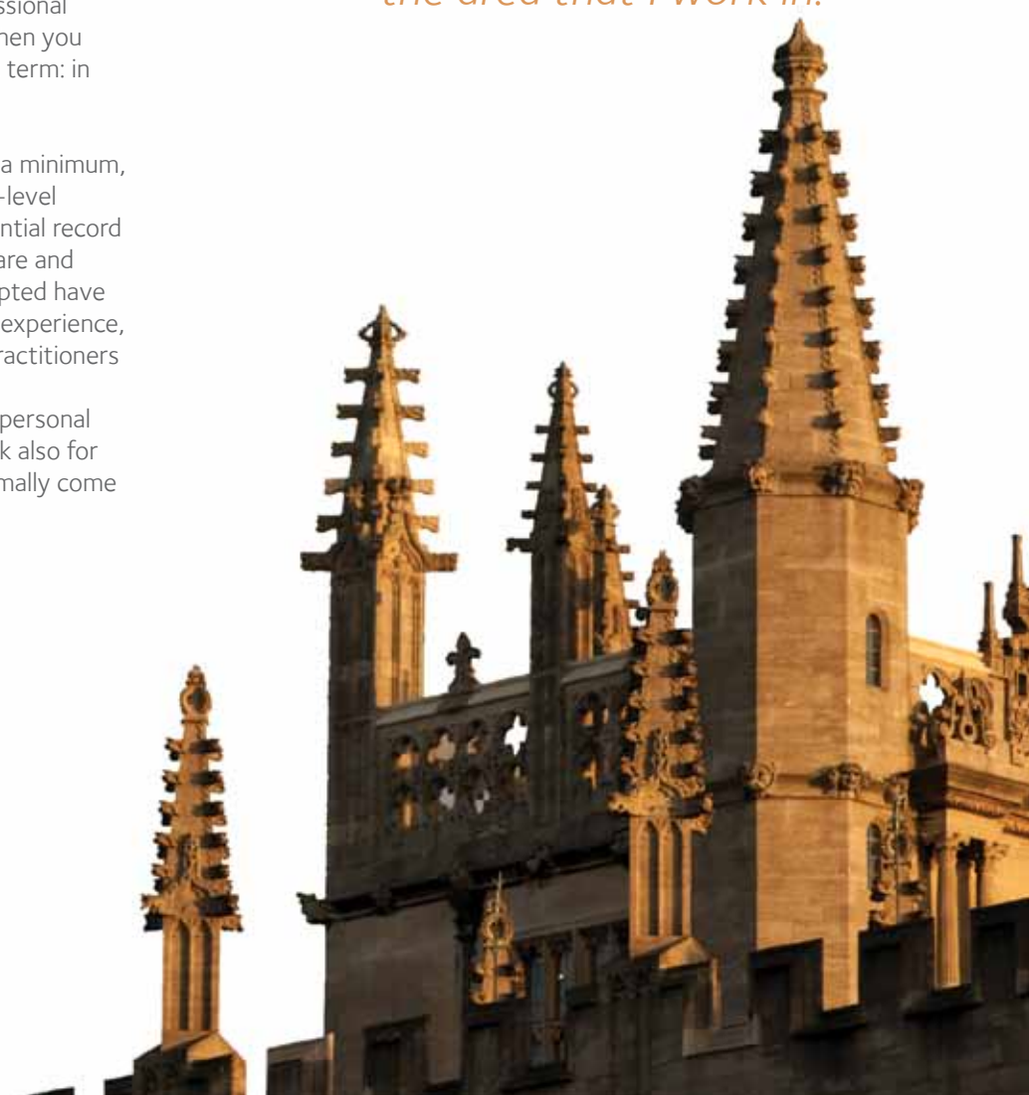
The admission criteria are straightforward: at a minimum, we expect applicants to have either a degree-level qualification in a related discipline, or a substantial record of practical achievement in the area of software and systems security. The majority of those accepted have both previous higher education and industrial experience, but applications are welcome from security practitioners without formal qualifications, and those with qualifications who have recently developed a personal or professional interest in security. We will ask also for at least two references, one of which will normally come from your current employer.

www.softeng.ox.ac.uk/apply

Course Selection

Each of the courses is designed to work as a separate programme of learning, and courses in related subjects can be taken in any order. Some of the courses assume familiarity with material taught in others: if you are not already familiar with this material, then you may obtain greater value by attending the other courses first. Advice and guidance on course selection can be obtained from the Programme Office.

"I work in IT, but my background is in physics. This was an ideal opportunity to get a formal qualification in the area that I work in."



Academic Awards

To be awarded an MSc in Software and Systems Security, you will need to attend ten short courses, complete the corresponding assignments, and write a dissertation based upon a research project of your own design. You have four years from the date of admission to do this, although more time will be allowed in exceptional circumstances. Most students take three or four years to complete the MSc; some take two years, which is the minimum period allowed between admission and graduation.

The majority of courses attended, and the topic of the dissertation, must be in the area of security: that is, chosen from the list of security courses. The remaining courses may be any of those offered by the Programme, addressing a wide range of subjects in software and systems engineering. If you would prefer to take the majority of your courses on subjects other than security, or if you would prefer to write a dissertation on a Software Engineering subject, then you can choose to be examined instead for the MSc in Software Engineering.

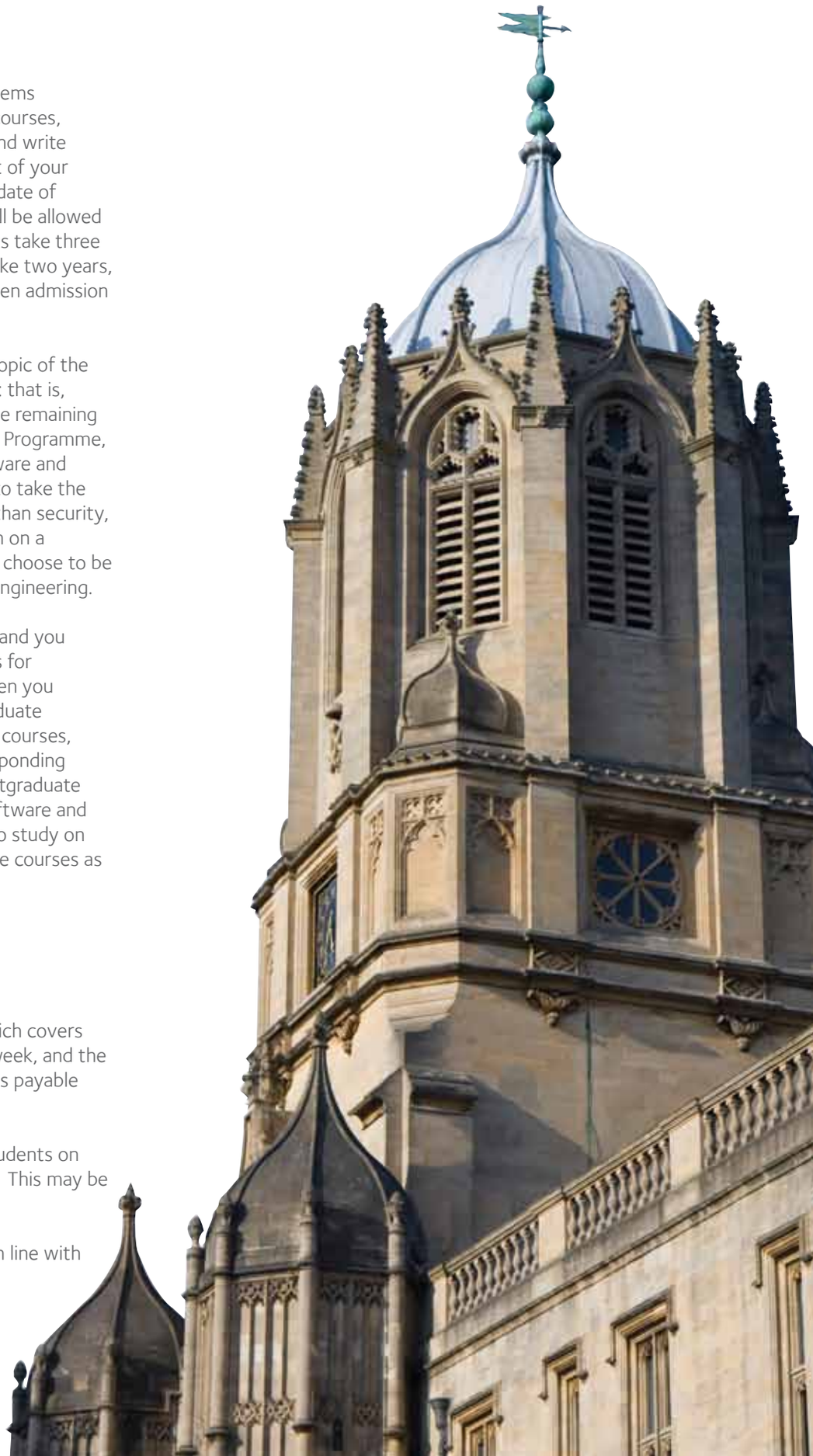
If your plans change while you are studying and you are no longer able to meet the requirements for an MSc, even if more time were allowed, then you may choose to be examined for a lower graduate qualification. Attendance at four (or eight) courses, and the successful completion of the corresponding assignments, can lead to the award of a Postgraduate Certificate (or Postgraduate Diploma) in Software and Systems Security. Should you later return to study on the Programme, you will be able to use these courses as credit towards an MSc.

Fees

There is a fee for each course attended, which covers materials and lunches during the teaching week, and the assignment, but not accommodation. This is payable strictly in advance.

There is an additional registration fee for students on the MSc in Software and Systems Security. This may be paid in up to four annual instalments.

These fees are revised each year, typically in line with the rate of inflation in the UK.



Key Facts

- a flexible programme in software and systems security leading to an MSc from the University of Oxford
- a choice of 30 different courses, each based around an intensive teaching week in Oxford
- MSc requires 10 courses and a dissertation, with up to four years allowed for completion
- applications welcome at any time of year, with admissions in October, January, and April.

Contact

Software and Systems Security
Oxford University
Department of Computer Science
Wolfson Building
Parks Road
OX1 3QD UK
+44 1865 283525
security@softeng.ox.ac.uk
softeng.ox.ac.uk/security