

The University

The University of Kent at Canterbury is built on 300 acres of parkland in the midst of the Kent countryside on a hill overlooking the city. Founded in 1965, it combines modern architecture with open green spaces, courtyards, gardens, ponds and woodland which, put together with the view across Canterbury and the Stour Valley, make it an attractive and friendly campus.

Biometrics Laboratory



DEPARTMENT OF ELECTRONICS

MSc Information Security & Biometrics *at Kent*



The Kent Experience

being a student at Kent is not just about studying for your degree; it's about the whole Kent experience including:

- high-quality teaching
- a cosmopolitan community
- attractive campus situated close to London and continental Europe
- excellent services and facilities
- work and volunteering opportunities
- strong industrial links
- degree ceremonies in the historic setting of Canterbury cathedral

How to Apply

Please contact our Postgraduate Admissions Officer, Dr Gareth Howells, for an application form; or you can apply online.

For more information visit the postgraduate prospectus web pages and/or contact:

Dr. WGJ Howells
Postgraduate Admissions Officer
Department of Electronics
University of Kent
Canterbury
Kent
CT2 7NT

E-mail: ee-admissions-pg@kent.ac.uk

Web: www.ee.kent.ac.uk



Secure information systems are critically important to modern day businesses and societies. Whether they be banking systems, medical systems, power infrastructures, or a simple home PC, ensuring their security is vitally important since they are usually all interconnected directly or indirectly via the Internet or telephony system.

Biometrics-based security techniques – identification and verification using human characteristics and behavioural traits such as fingerprint and iris recognition – are playing an increasingly important role in securing information systems and physical assets, both in government and industrial contexts, especially in the aftermath of recent terrorist attacks, identity theft and Internet-based fraud. There will be a long-term need for expert professionals trained to a high level in order to meet the rising market demand.

Staff at the University of Kent have been among the pioneers of biometrics and public key infrastructure (PKI) research in the UK, and have an established reputation for developing and testing these systems. The Department of Electronics has a strong and widely established reputation for its work in various aspects of biometrics, including individual biometric modalities, to study techniques for optimal integration of biometrics, to manage the complexity arising from the design of flexible biometric systems, and in the testing and evaluation of biometrics, image analysis and some key application areas.

Staff in the Computing Laboratory have been at the forefront of distributed systems and PKI research, participating in the development of the X.509 international standard and being the first group in the world to build an X.509 privilege management infrastructure (PMI). They were also one of the first groups to pilot PKI systems with the NHS. We therefore maintain a balance between the development of essentially generic techniques and application-led work in important areas of biometric and PKI/PMI technologies.

MSc PROGRAMME

This Masters programme offers an advanced level of learning by providing students with a thorough understanding of the theories, concepts and techniques for the design, development and effective use of secure information systems, and producing graduates who are capable of adapting to changes in the field and leading it in innovation. The course is designed for practitioners, professionals and graduates with an interest in information security, access control technologies, and application domains using biometric identification and verification systems.

COLLABORATION WITH INDUSTRY

Both the Department of Electronics and the Computing Laboratory have strong industrial contacts which will be used extensively to deliver and enhance the course. One module will explicitly include a number of industrial seminars presented by invited speakers to update students with current state of the art techniques and problems.

Significant project support from industry is also envisaged, either within the University or as industrial placements at the host institution. These collaborations will be further enhanced via an industrial liaison panel, comprising members of the university directly responsible for the provision of the course and representatives from the industry.

MODULES

The course is taught in 4 compulsory modules and a choice of a further 2 out of 4 options, followed by a five month project with significant industrial involvement:

Foundations of Biometrics and Secure Systems

An introduction to biometrics and biometric systems giving the student an overview of a number of biometric modalities. This is combined with an overview of pattern recognition techniques, an introduction to programming, and data analysis techniques required for the development of biometric systems.

Object Oriented Software Engineering

A detailed study of the use of Object-Oriented analysis and design methods to analyse problems and design solutions, and the impact that these methods have on development lifecycles, including a comprehensive introduction to the UML notations and their applications to real-world problems. Object-Oriented Java Programming including Java roots, structure of the JDK, www and security issues, overloading and overriding, memory management, inheritance and dynamic binding, nesting versus inheritance, abstract classes versus interfaces, finalization and final things, polymorphism, packages and protection levels, deep-copying, exceptions, callbacks, inner classes and anonymous classes.

Internet Security

An introduction to Internet technologies including TCP/IP, DNS, LDAP, SMTP and HTTP followed by a comprehensive description of symmetric and asymmetric authentication techniques including digital signatures and one time passwords. Web services, single sign on, SSL, firewalls and web services security are also covered.

Practical Biometrics

A detailed treatment of the implementation of biometric systems including examples of systems using the major modalities and an analysis of modality specific features and feature extraction, selection and classification strategies. State of the art in sensor technologies; spoofing and counter-measures; analytical approaches to the performance of biometric systems; biometric encryption and an introduction to BioAPI are also included in this module.

Advanced Biometrics (option)

This module introduces advanced methods for pattern recognition with emphasis to multibiometric systems. A detailed analysis of the Bayesian classification framework is followed by an introduction to error estimation and advanced feature selection and extraction techniques. Multiple classifier systems, including intelligent and dynamically adaptable classifier combination strategies, such as genetic algorithms, are studied as the basis for the development of state of the art multibiometric systems. A discussion of score normalisation methods and the use of soft biometrics is also included in this module.

Trust, Security and Privacy Management (option)

A systems level view of information security management, including ISO 17799, risk management, legal and usability issues is provided. Various security models (Bell and LaPadula, BIBA etc) and middleware architectures are described. Trust management, trust negotiation, trusted platform modules, and policy based systems are described. Data privacy, authorization, and various privacy and security policy languages are introduced, as well as the concepts of steganography and digital watermarking.

Industrial context of Biometrics: Standards, Testing, and Evaluation of Biometric and Secure Systems (option)

This module provides an examination of the importance of standards and regulation in biometric systems and examines associated standardisation bodies and procedures. Issues related to data collection, volunteer sampling and ethical issues are also addressed. The module is accompanied by a significant number of industrially led colloquia introducing students to the current industrial context for the course. The modules are taught in sequence with significant practical experience at each stage.

Mobile and Ubiquitous Computing (option)

An introduction to mobile, context aware, ubiquitous and pervasive computing and a comparison with conventional

computing environments. Handheld, wearable, embedded and sensor devices. Characteristics, limitations and constraints of hardware and software. Service/Device/Person discovery, Location based services, Sensor networks Programming environments HCI issues including interacting with small devices, matching interaction modes and avoiding interactions. The modules are taught in sequence with significant practical experience at each stage.

PROJECT

The project will provide practical experience of the design of a significant biometric or information security system. Many projects will involve working closely with an industrial collaborator which will provide experience of secure systems design in an industrial environment and allow students to appreciate the practical difficulties in the development and utilisation of such systems. Students will be able to demonstrate ability in generating, analysing, presenting and interpreting data, will learn to employ the software engineering and system development skills they have acquired and will develop core key skills, such as learning effectively, critical thinking and time management.

STUDENTSHIPS

The programme is well-supported by companies and research establishments in the UK and overseas. It continues to be supported by EPSRC Collaborative Training Account studentships. For information on our various studentships, bursaries, etc, please see our pages on www.ee.kent.ac.uk.

ENTRY REQUIREMENTS

A good honours degree in Electronics, Computing or a subject with a strong IT component, although allowance will be made for significant professional experience.

The University requires all non-native speakers of English to produce evidence of proficiency in written and spoken English. We require a minimum score of:

- 6.5 in International English Language Test (IELTS)
- 600 in paper-based or 250 computer-based Test of English as a Foreign Language (TOEFL)
- 'B' in the Cambridge Certificate of Proficiency in English
- 'A' in the Cambridge Advanced Certificate in English

COURSE FEES

This course can be undertaken on a full- or part-time basis; please contact our admissions officer for further details.