**University of Oxford**
**Computing Laboratory**
**Software Engineering Research Group**

Applications are sought for a fully-funded EPSRC CASE studentship supported by QinetiQ in the area of **usable secure software engineering.** This project aims to explore and research the modelling of system environments in order to support both usability and security needs.
The intention of the CASE scheme is to give the student an opportunity to work closely with the industrial partner. During the course of their studies, the student will spend three months working on site at QinetiQ. The company will help in providing direction for the research, motivated by known and emerging problems, and case studies where appropriate. In turn, QinetiQ will also help to find ways to exploit the results of the project.

**Project Summary**

In the field of safety-critical software engineering, research into understanding and modelling the environment of an operational system has been ongoing. This research has yielded insights into the properties of environments that contribute to systemic failures, leading to eventual safety violations.
"Unsafe systems can result from incorrect assumptions about the environment in which the system will operate. (...) Precise environmental modeling is a great asset in developing such systems and in determining realistic, operational test cases." [Lutz]
Whilst similarities exist between the fields of safety and security, such as the goal of reducing high risks, there are also significant differences. Possibly the most important of these is that security has to consider a malicious and intelligent adversary, whereas safety generally contends with random failures (which are significantly easier to model statistically). Another significant advantage the field of safety holds over that of security is the availability of good data about safety failures. Such data is almost never available in security, which directly impacts the usefulness and ease of use of risk analysis tools.
This is not to say that insights gained from safety research are not applicable, however there is a need to further explore and research how these might apply to security.
In addition to this, the growing field of usability research in computer security has been highlighting the importance of developing systems that are not only secure, but usable. The argument was originally made in 1975 with the principle of psychological acceptability for computer information systems [Saltzer & Schroeder]. This principle highlights that where people are an important part of the security of a system, a security system that is hard to use is much more likely to fail.
The AEGIS methodology [Flechais et al.] has explored integrating usability and security into a coherent design strategy. One of the core principles of AEGIS, adapted from the field of Human Computer Interaction (HCI), is the need to understand the context of operation in order support design decisions that fit this environment.
One of the outcomes of this research has been that understanding and modelling the context of operation could have a significant impact on important factors in system operation and design, such as:

- task performance
- cultural effects
- motivation
- threat profiles
- risk mitigation strategies
- recovery measures

In principle, research into modelling the operational environment of a system could lead to significant insights into designing and deploying security solutions that are effective at mitigating risks and appropriate to their context of use.

### Selection Criteria

Candidates must satisfy the usual requirements for doctoral study at Oxford:

`http://web.comlab.ox.ac.uk/oucl/prospective/dphil/dphil-criteria.pdf`

Applicants should have a strong background in software engineering or computer science and should have a BSc or MSc degree in an appropriate discipline. They should be strongly motivated to conduct original research and with the personal skills required to work closely with our industrial collaborator.

Applicants MUST meet the EPSRC eligibility requirements which state that you must have a relevant connection to the UK, generally established by 3 years residence. On-site working at QinetiQ will also require obtaining clearances, which may be based upon nationality.

### How to Apply

The deadline for applications is 16th July 2007. Interviews for qualified candidates will follow soon afterwards, if necessary. To apply you need to download the University's application form from:

`http://www.admin.ox.ac.uk/postgraduate/apply/forms`

You will need to submit references and a transcript with your application. It is also required to submit a research proposal: in this proposal, please elaborate on the reasons why you are interested in this project, and the research questions you find most exciting and important to address within the scope of the project.

Please submit your application to:

Mrs. Julie Sheppard
Secretary for Graduate Studies
Oxford University Computing Laboratory
Wolfson Building
Parks Road
Oxford OX1 3QD
United Kingdom

*AND NOT TO THE ADDRESS ON THE APPLICATION FORM*

### Further Information

For informal enquiries and further details, please contact Dr. Ivan Flechais by email at `ivan.flechais@comlab.ox.ac.uk`.

### Further Reading

Robyn Lutz, "Software Engineering for Safety: A Roadmap". In "The Future of Software Engineering", Anthony Finkelstein (Ed.), ACM Press 2000.

Jerome H. Saltzer and Michael D. Schroeder, "The Protection of Information in Computer Systems", Fourth ACM Symposium on Operating System Principles, 1975.

I. Flechais, "Building Secure and Usable Systems". PhD Thesis,
`http://www.softeng.ox.ac.uk/personal/Ivan.Flechais/publications.html`

I. Flechais, M. A. Sasse & S. M. V. Hailes, "Bringing Security Home: A Process for Developing Secure and Usable Systems". ACM/SIGSAC New Security Paradigms Workshop, Switzerland, August 2003.