File 20110417.1939: New GSO.14 narrative:

Please give a brief indication of the nature and progress of your research to date.

Looked at narrowly, this research solves a particular problem in security: the cost—in both time and funds—of required security evaluation and pre-connection accreditation of Cross Domain Systems (CDS) is excessively large. Too narrow a focus, however, disregards the important generalisation beyond classified government and military applications to civil, commercial and privacy-respecting information systems as well. But this is still too restricted a view of the landscape; in a more general sense—and this assertion is supported by evidence—the CDS security approval bottleneck is a systems integration problem comprising people, things, risk, and processes. The problem has roots in the literature of engineering failure analysis, information security standards, testing, risk assessment, philosophy of risk management, phenomenological research, history and economics. A wide range of different areas of specialisation had to be explored before a gestalt began to emerge.

The thesis is founded on three case studies centred around software implementing a controlled interface for classified information in the US and UK governments. In each case study, a particular embodiment of similar software was required to undergo security evaluation and certification testing for use in a particular environment. In one case study, the certification criteria were the Defence Information Assurance Certification and Accreditation Process (DIACAP). In another case study, the Common Criteria for Information Technology Security Evaluation (CC) scheme was used. The final case came under Director of Central Intelligence Directive (DCID) 6/3. One of the security evaluations proceeded successfully to certification; another was inconclusive, and a third was abandoned in failure after the expenditure of millions of dollars and years of work. The original conception of this research was to find out why the first case study failed. After additional data on more case studies was found in the course of research, the direction shifted to developing a possible solution to make future security evaluation activities more likely to succeed. Late last year, however, it emerged that the foundation of any proposed solution would be better served by careful re-analysis of the original data using grounded theory methodology. The researcher believed incorrectly that the data were valueless because of the participant–observer relationship; in December it was made clear that in fact this trove contains extremely valuable data that must be published for other researchers to access. This explains the recent change of direction in research.

Beginning immediately in January 2011, grounded theory methodology and related research techniques in qualitative analysis were studied. Grounded theory analysis of the first case study is underway now and expected to be completed satisfactorily before the end of Trinity term. Written evidence and three or four completed chapters for confirmation of status will be available in the summer.

Your proposed timetable for submission:

A detailed Table of Contents for the entire dissertation extending down to approximately the paragraph level exists at the time of this application. Chapters 1 (introduction), 2 (literature survey) and 3 (methodology) had to be rewritten in whole or in part as a result of the change to grounded theory methodology. Chapter 4 (the first case study) will be written during Trinity and provided to the assessors before the end of the term. Their feedback on the content of that chapter will guide and improve Chapters 5 and 6 on the remaining case studies. Those chapters are expected to take approximately four months from August 2011, extending to the beginning of December. Chapter 7 (interpretation) and Chapter 8 (summary and conclusion together are expected to require six weeks from 1st December, for on-time submission of the completed dissertation by 13th January 2012. The appendix is essentially complete now; it was accumulated at the time of publication of the VALID 2010 conference paper last year.

References