File 20101123.1530: Draft of GSS report:

How many times have you met with Dr Andrew Martin since your last report? 9

Do you have any concerns about the progress of your course over the last reporting period? no

Self-assessment of overall progress this term: Use this space to describe your progress including details of work completed and the current focus of your study plus any concerns you may have. [4000 characters]

Primarily two activities comprised the bulk of progress this term: data collection and further development activity on the numerical model of inter-accreditor communication. In return for minuting their meetings, access was obtained to a series of classified telecons amongst the software developer, government programme office, certification authority, penetration testers and independent verification and validation contractors of the second case study during factory acceptance testing, government regression testing, certification test & evaluation and security test & evaluation of the system designated 'R-double-prime'. Participants were observed interacting and in some cases interviewed outside the meetings to clarify particular observations. The process was followed beginning with the certifier's decision to use NIST SP 800-53 evaluation criteria for the first time, through successful accreditation at USSTRATCOM, deliberation of the CDTAB board, and issuance of the UCDMO baseline configuration for TSABI approval. Several meetings with a former DAA, the programme manager and government sponsor were made to arrange access for interviews with a set of working accreditors, but permission was unexpectedly withdrawn. Denied access to that source of information, it was necessary to adapt the research methodology to a new direction. Rather than proceeding with the original plan of interviewing practitioners, instead a numerical model of inter-accreditor communication was developed based on a theory of asymmetric knowledge and information flow patterns observed in the first and second case studies. It was proved that the inter-accreditor communication model satisfies Spence's (1973) criteria for signalling and Akerlof's (1970) requirement that signals must be expensive to be effective. Several attempts to model the theory were tried and abandoned before settling on a physics-based analogue able to be simulated using an arrangement of springs, fixed points and masses representing accreditor risk decisions, risk tolerance and accreditor influence, and hazard ratings, respectively. Experiments on the model are being done in MATLAB with the Simulink and Simscape libraries. The model, with accreditors having different security clearances, and risks and risk mitigations being classified at different levels, is sufficiently general to represent intra-national inter-service, international and SCI accreditations of cross domain systems, thereby covering the gamut of situations encountered in the real world. Interpretation of the meaning of several physical parameters and the trajectory of masses in phase space are being studied and compared to observations made in the first and second case studies; discussions with participants and DAAs tend to validate that predictions made from the model are applicable to real CDS accreditations. The discipline of regular status reports and supervisor meetings has been maintained. Written work (four papers, only one of which has been published so far) and a confirmation report were submitted to the assessors at the end of October; a confirmation viva is scheduled for 16th December. Travel arrangements to Oxford have been made.

Training attended: Comment on subject-specific or generic skills which you have acquired during the previous term and on any training courses which you have attended, e.g. attending and giving papers at departmental seminars, seminars/workshops on giving presentations, training in using bibliographic software, training courses in laboratory techniques etc. [1000 characters]

A paper on methodology and preliminary results obtained from two case studies was presented at the 2nd International Conference on Advances in System Testing and Life Cycle in Nice, France. A second paper describing the asymmetric knowledge problem (but without an inter-accreditor communication model that solves the problem) was submitted but rejected by the 2nd ACM Workshop on Assurable and Usable Security. An extended version of that paper is currently in preparation for submission to the 10th Workshop on Economics of Information Security. Other talks this term were given at Lockheed Martin to audiences on the topics of: technology for copyright and privacy protection, TEMPEST (twice), crypto maths and DoD 8570.01-M. Co-taught a ten-week CISSP exam review course for Lockheed employees. Member of the COMLAB-CS-2010 programme committee. Training obtained this term ranged over economics, risk assessment, U.S. government procurement, secure coding, MATLAB, physics, statics and mechanics.

Training required: Use this space to comment on subject-specific or generic skills which you would like to acquire and on any training courses or seminars you would like to attend. [1000 characters]

More time for reading is needed. After difficulty implementing the physics model as a control law system in MATLAB was encountered, a newly released optional library called Simscape was found that

greatly facilitated the work. Time to go through the numerous video tutorials for Simscape is in short supply.

References