File 20101017.1237: Notes for GSO.14 form:

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

The path of my research has evolved, but never its aim. The problem has always been that the high cost of Certification and Accreditation (C&A) activities is delaying the operational deployment of necessary systems between and within the U.S. and U.K. governments. I set out to solve that problem.

Beginning in 2007 with a fairly simple question ('why did this Common Criteria security evaluation fail and how could we do better in future?') the search for a solution has proceeded backwards into history and forward along with the evolution of improved standards. In 2009, the Director of National Intelligence announced that NIST Special Publication 800-53 would form the foundation of the next Certification Test and Evaluation (CT&E) effort. I moved house and took a new job with Lockheed Martin to obtain access to the first programme that would go through the new DIACAP process. It became my second case study.

At the time of Transfer in early 2009, I was planning to collect additional data from an ethnomethodological study of U.S. and U.K. government security accreditors. It would inform the design of a tool intended to improve inter-accreditor communication. The tool was to be validated against the historical project data from two case studies before being applied on a live project.

Communication indeed turned out to be the root of the problem, but not for the reasons I expected. Government accreditors in both counties repeatedly declined to cooperate, citing legal difficulties. It appeared I would be without an important source of data. Not an uncommon occurrence in science, but under the circumstances it demanded adaptability.

Earlier this year I began developing an abstract model of accreditor behaviour that would be sufficiently general to encompass the important problems of the field but simple enough to simulate numerically. Looking around for a principle upon which to base the model, I found it in economic theory—specifically the problem of asymmetric information. In the course of validating the applicability of the model, I proved an interesting result: that the criteria for Spence's (1973) theory of job market signalling were precisely satisfied by my abstract model of accreditor–accreditor interactions. This suggested the idea of a risk market.

At present, the model is implemented by a system of differential equations in MATLAB simulating the physical analogue of an artificial risk market in terms of fixed points (representing accreditor position along a continuum of risk tolerance), moving masses (representing risk mitigationss proxied by the amount of work needed to mitigate a particular risk) and springs stretched between them that represent bid/ask prices. Removable pins fix the initial position of each risk according to the determination of baseline risk by a certification authority. When the pins are pulled, risks follow a characteristic trajectory suggestive of events observed in the second case study. It is hypothesised that in the absence of a priori knowledge of the spring constant k, it should be possible to predict the lowest-energy configuration of a set of risk mitigations (that is, the total residual risk acceptable to all accreditors) from three measurements along each of their orbits, thereby short-circuiting a negotiation process between developer and accredtors that today requires years.

I have published the methodology but not yet the risk market solution. I expect that finalising the model and running experiments on it will take five months, allowing me to finish writing up before the end of Hilary term 2011.

'Your proposed timetable for submission:'

Chapters 1 (Introduction), 2 (Literature survey) and 3 (Methodology) are essentially done. Chapter 4 (Evidence) is expected to take five months from November 2010; this work comprises further development and experiments on the numerical model, documentation of the precise sequence of events in each case study, and statistical analysis using R.

Chapter 5 (Interpretation) is expected to require six weeks from 1st April 2011, plus writing time. Chapter 6 (Summary and conclusion) is expected to be completed by the end of May. Appendix A is essentially complete now; Appendix B is in a file that is accumulated as the project moves along.

Barring unexpected delays, I plan to submit before the end of Trinity term 2011.

‘Please describe briefly any subject specific research skills that you have developed or improved in the course of your time as a Research Student. For example, these might include: research methodology; data analysis and management; record keeping; bibliographical skills; presentation of research.’

> I began using an electronic laboratory notebook early in the process. It is searchable, remotely accessible, regularly backed up and version controlled. It is indispensible. From the beginning I have maintained a discipline of writing weekly activity reports to my supervisor. These together with a written agenda for every meeting and faithfully transcribed notes all go into the laboratory notebook. At my supervisor’s advice, I learned to use an on-line calendar and now depend on it.
>
> I passed the ISSEP examination, a certification for security test and evaluation practitioners in government. Fewer than 500 people currently hold this certification worldwide.
>
> I have read extensively in my time as a Research Student about methodology, statistics, writing, presenting and teaching, in addition to hundreds of papers, books, and government standards related to my thesis. All are citable by reference to my BibTex file. My library skills and familiarity with bibliographic databases have improved measurably. I make extensive use of interlibrary loan.
>
> I have gained experience with grant writing. At Lockheed I wrote three proposals, not something ordinarily done by persons in that job category. One of the proposals was funded: the U.S. Air Force Research Laboratory (AFRL) in Rome, New York awarded a contract for $800,000 over three years (enough to support two half-time engineers) for a cognitively assisted declassification algorithm. After a successful Phase II, I just sent a new proposal to DARPA asking to further develop the prototype into a multi-user tool and ensure continued funding. I would not have known how to do that before.

‘Please describe briefly any personal and professional skills in which you have received training or which you have enhanced during the course of your time as a Research Student. For example, these might include: time management; language skills; IT skills; team work; problem solving; presentation skills; teaching skills; career planning.

> I have self-studied MATLAB and SimuLink to implement concepts I took from books on economics and engineering mechanics (dynamics). I have greatly improved my experience and comfort level with public speaking. In addition to giving two Friday seminars in Oxford, I have done 14 one-hour talks to audiences of Lockheed engineers, on topics ranging from certification and accreditation standards, to my research, cross domain systems, secure deletion, TEMPEST signal processing and crypto maths. I traveled to France and presented a paper on certification to unstable criteria.
>
> I have had rejection letters. I submitted unsuccessfully to ACSAC, SafeConfig, and the 4th UCDMO Conference. Following the advice of DGS, I have selected conferences to maintain about a 1:3 ratio of acceptances to rejections, indicating about the right level of risk-taking.
>
> I participate regularly in the Security Reading Group, having introduced my fair share of papers. I presented a paper at the 2008 Comlab Student Conference, then helped run the programme committee this year.
>
> I have begun to think about teaching and about applying for a postdoc research fellowship.

‘Please identify any subject-specific or personal and professional skills in which you (and your supervisor) forsee the need for fuuther development or training.

> Time management and software estimating. More practice in public speaking.

‘Please list any other activities which have contributed to the development of your work. For example, these might include courses attended, conference presentations given, publications, opportunities to undertake teaching, etc.’

> I attended four Software Engineering modules (SDE, SCS, DES and REN) either because I wanted to take it or because I thought the course would be useful. I attended the LASER summer school in Italy and tutorials at conferences in Oxford, San Diego, Nice, Washington D.C. and London.

Note: the above answers got modified a bit into the final GSO.14 form. Forms submitted to Dr Martin on Sunday night; Julie Sheppard replied to my email that she would shepherd the forms over to St Cross College for their stamp of approval, yay.

References