File 20100719.0804: Notes from meeting with Dr Martin this morning:

I began by referring to the updated agenda I sent out last night with more details. I have been working on a numerical model for the pricing function that I need to prove that the accreditor–accreditor interaction model behaves like a market. To this end, I have a catalogue of six hundred security controls from the NIST SP 800-53 standard and I am starting to go through the list and rank-order them by the amount of effort or pain and suffering required. I do not know how to assign an absolute numeric value to them yet, but for a start I can at least establish a partial ordering. I want the price to reflect the amount of work that an accreditor would have to do, or conversely the amount of work they would not have to do if another person pre-empted that test by doing it first or offering to do it instead. It might be useful to implement the concept of promising to do such work in future, perhaps even with a discounted 'net present value' type of relation to value work that has not been done yet. I should build this in to the model.

Dr Martin said he is still trying to decide what to think about it. He wondered if it might evolve into a more complicated bit of game theory later on, that a simple numerical equilibrium might not be all that is at the core of it, once I really understand it. Make sure that the incentives fall in the right places. (This is actually one of the tests that a proposed equilibrium is really an equilibrium.) I suggested that turf wars, something I have already noted the existence of, might be one of those complicating game theory factors.

I had an interesting conversation with a retired Air Force accreditor last week (Steinberger). He and I discussed the ways in which a tool such as the one I propose could have made his job easier. All of the accreditors I have talked to so far (e.g., or i.e., Ozura) have said the same thing: if I can figure out how to get the other guy to do the work, they are in favour of it. Dr Martin pointed out that fairness is important: it would not do to dump all the work on the little guy. I agreed that there should be a concept of fairness in the tool, and related a lecture by Professor Polak at Yale that I watched the other night, in which he described an example where unfairness was structural. Despite the fact that the equilibrium he showed was more efficient than the case with no equilibrium, it was inherently unfair: the lowest-paid participants ended up getting paid 30 in the more efficient equilibrium, whereas they were paid 32 in the less efficient equilibrium. The richest were not paid any more, but the poor were paid less. The difference went to waste. It was an interesting lesson. I will try in my tool to get everyone to do a lot of the work, but efficiently. More efficiently than at present, anyway. My two case studies will be useful as baselines to show what 'at present' means.

We looked at my three-month goals. My first and most important goal is to develop the 'equilibrium' model further to the point where I can begin to implement some of it. Dr Martin pointed out the difference between a model, on which I can perform experiments and do what-ifs, and the implementation a tool for real accreditors to use. Dr Martin cautioned against trying to make it over-general, that I could spend all my time implementing. I discussed investigating use of systems engineering modelling tools. I know they exist, but not how to use them. I would like to avoid reinventing the wheel if possible. Dr Martin said that looking at modelling tools would be a good idea. Are there any free ones?

My second three-month goal is to finish the analysis of the failed EAL 4+ evaluation. I discussed whether to try to use it to argue the case that if my proposed too had only existed beforehand, the evaluation might not have failed. Dr Martin commented that the argument is not falsifiable. It is all right to hint at conclusions, but primarily I should presrnt my data and conclusions, and let the reader decide the significance. It is still okay to hint, however.

The third goal for the next three months is to write up a similar analysis of the RM 5.0 CT&E effort. It would not be a contribution, however, simply to describe what happened. I need to explain why things happened. I have been taking careful notes of the meetings I have been in. I reported current status; I think they will probably slip the schedule three weeks, making the certification date the first week in September, but I do not think they will run out of money and I do not think the penetration testers will spring any surprises. I have certainly seen a lot of interesting human interactions, only slightly constrained by the relevant standards documents.

The purpose of these three goals is to have preliminary results to show to the assessors at confirmation of status. I may not get to the EAL 4+ analysis before then. I have all this data to analyse, but it may have to wait until after confirmation.

Dr Martin will be in Australia for the next month, but reachable, at least on a few days notice. I have a good plan and a lot of work to do, so I am going back to work now. I am going to work on the pricing algorithm, the surveys, and the Crosstalk journal article.

Dr Martin said it is coming together pleasingly.
Call ended 0725.

References