File 20090116.1630: viva voce after-action report:

The first words I heard when I stuck my head in the door, right on time, were, 'Go walk around the block. Give us five or ten minutes.' So I did.

The assessors were Dr Marina Jirotka and Dr Andrew Simpson. I started out by speaking for a few minutes about where I came from, where I am, and where I am going. On the whiteboard I began to draw the landscape of certification and accreditation programmes and their interrelationships including people, organisations, countries, and standards. The discussion wandered a bit, but I managed to cover all the points I wanted to make.

Dr Jirotka said I need to substantiate my claims [which I was careful to explain were anecdotal] that the Common Criteria (CC) process is broken or not working well.

We discussed the differences between a Retrospective Study (studying the records of the RTG failure) and an Ethnographic Study (watching in real time another CC evaluation project as it takes place). We agreed that I probably do not have time enough to do an ethnographic study, so retrospective it is. There is a third type of study, a participant study, where I would myself participate in a new CC evaluation—using my new method—to validate the new method.

Validation of the new automated method I propose is crucial to my thesis. It is not enough merely to develop a new tool; I should attempt to validate it and show the results. Even if my new method should prove completely inadequate to the task, that in itself might be an interesting result, to the extent that it leads to the discovery of something else that works.

Dr Jirotka suggests two case studies, not just one. First, a survey of people's opinions of the CC. That should be relatively quick and easy to do. Second, a retrospective case study of what happened in the RTG effort. That's called documentary analysis. I will go talk with Dr Jirotka to get the jargon right.

Dr Simpson asked me some questions about the way the national schemes work and the persistent rumours of 'evaluation shopping' because some countries are known as 'easy graders' in the community. Ross Anderson actually says it in his book. I answered that honestly I don't want to touch that question with a ten foot pole. We agreed that it's not part of my study and Dr Simpson expressed some relief that I'm not planning to go there.

Dr Simpson told me that my writing style is not up to proper academic standards. Actually, they said it was 'rubbish'. I concurred, and explained that I will write the eventual thesis in a more formal style. I presented a copy of my 2002 article in ACM Trans. Info. Sys. Sec. as evidence that I can write in that style when necessary. The assessors said that the structure of my transfer report is confused—I agree—but they're not going to make me rewrite it or make changes. (The reason it's rubbish is because the first draft was 89 pages long. My college advisor helped me out a lot (really) by attacking it with a vicious red pen. Entire sections came back crossed out with 'Inappropriate!' and 'DO NOT SAY THIS' scrawled across the pages. The report that the assessors read was missing those bits; it was much, much better than my first draft. Thanks, Dr Ashbourn for your help editing!

We then discussed the automated tool that I will produce. I was somewhat surprised that the assessors did not give me a harder time over that. My design is not well developed yet, and I was prepared to fight over it. Instead, the assessors (although they did not say so in so many words) seemed to be thinking either (1) 'of course you want to build a tool; every grad student wants to build a tool', or (2) 'sure, go ahead and build it; it won't work, they never do'. I'm not sure what the assessors were thinking. Maybe they're used to seeing very preliminary designs at this early stage in a DPhil student's research. Whatever the reason, they seemed much more interested in and enthusiastic about my case study. Dr Simpson even said that this will be highly significant research some day.

The only thing they were adamant about was that validating the automated tool is important. There was some slight misunderstanding, I felt, for a few minutes, over whether the automated tool I was proposing would be applicable to more than just the software system in my case study. I really felt that there was a misunderstanding there, so I pushed back hard a couple of times until the misunderstanding was completely resolved. The tool I am proposing is generally applicable, not just to the case study. It is completely disjoint from the case study.

That led naturally into a discussion of how to validate the new tool. They asked how I planned to do it. I proposed two methods: first, to choose a relatively small open source software programme (as an example I used OpenSSL), run the new tool over it to generate a complete set of CC work packages, then submit those to a Common Criteria Testing Laboratory and attempt to get it evaluated at EAL2 or EAL4+. Second, alternatively I could offer to my employer to get CC validation for one of its own internal products, instead of an open source programme.

Question from the assessors: who would pay for the testing lab's services (a significant amount of money, at least tens of thousands of pounds)?

Answer: my employer. Question from the assessors: wouldn't the payer want the intellectual property rights? That might not fly with OpenSSL.

Answer: instead of my employer paying, I could go out and apply for a National Science Foundation grant by myself. That seemed to please the assessors. It feels to me like, 'grow up and be a real scientist'. I reiterated that I really want to publish these results in a good conference and teach other practitioners how to use it. So intellectual property issues are important. (Note: might the University even try to assert an intellectual property claim? They might.)

Dr Simpson commented that my idea for an automated tool sounds like something that Jim (Davies? Woodcock? See page **??**) would say should be extended all the way to automatically generating software, not just documentation. I agreed that I'd thought about that but it would have to be future work.

Next the assessors asked me about funding. How did I plan to pay the cost of interviewing all these people? I answered that I think I can piggyback visits to the people onto regular business trips that I normally undertake for work. The participants are geographically clustered (New York, Washington D.C., California, and Colorado), and I see most of them face-to-face occasionally. The assessors seemed okay with this answer.

The assessors asked me what the 'residency requirement' on my schedule (Gantt chart, page 39) was. I explained that the University requires DPhil students to spend two years (six consecutive terms) living within a certain number of miles of Carfax tower, but that after that time I expect to return home to the USA where it's considerably cheaper for me to live. The assessors asked if I plan to remain a full-time DPhil student? Yes, I plan to remain a full-time DPhil student through 2009 and 2010. I am working part-time for Lockheed Martin now, and I plan to continue that arrangement through the end of 2009. At the beginning of 2010 I will go back to working full-time, although still remaining a full-time DPhil student (living pretty far off-campus). I hope to finish my research by the end of 2009, spend 2010 writing, and graduate at the end of 2010. (Note to self: update the Gantt chart to reflect reality again.)

Dr Simpson noted that I managed to crowbar one of his papers into my bibliography. I said that it seemed relevant in relation to Stoneburner's paper (2008) about applying safety-critical principles to security-critical systems, which ties in to what Mark Vanfleet of NSA has been telling me for years about MILS (Multiple Independent Layers of Safety/Security), and MILS is directly related to the recent achievement of EAL6+ certification by Green Hills Software, Inc. for their new operating system under the Common Criteria, which is used in the new F-35 fighter aeroplane, being built by my company. So it all ties together, see? I wasn't just citing your paper to crowbar it in there, all right? :-)

Finally, Dr Jirotka suggested I change the title to something like, 'Towards an Automated Process for Common Criteria Evaluation: A Case Study of...'

They're going to recommend that I pass. I will get their report in a few days, although it might take a long time to work its way through the bureaucracy.

References