File 20101217.1157 (GMT): Weekly activity report 0167:

weekly activity report 167 (loughry)
Joe Loughry
Sent: 17 December 2010 11:57
To: Niki Trigoni; Andrew Martin; Joanna Ashbourn
Cc: Ivan Flechais; Marina.Jirotka@comlab.ox.ac.uk; otaschner@aol.com;
anniecruz13@gmail.com; andrea@hpwtdogmom.org;
chip.w.auten@lmco.com; edloughry@aol.com; diane@dldrncs.com;
Joe Loughry; mmcauliffesl@comcast.net; tom.a.marso@lmco.com

Weekly activity report no. 20101216.1320 (GMT) sequence no. 0167, week 8+2 MT

Copied to Dr Jirotka and Dr Flchais in addition to the usual recipients.

Travel to the UK was uneventful, although the Atlantic crossing was rough air the whole way. The majority of activity over the past seven days is irrelevant now because of the redirection received in the viva yesterday, but the following historical time-line is relevant:

* ca. 1999: the AEHF project requested a Common Criteria documentation set to be 'evaluatable at EAL 4'. Historical records from this project comprise case study number 3, designated R-zero.

* 2004--5: the R-prime project failed to achieve Common Criteria evaluation. This was the original case study.

* 2006: First research proposal. The original purpose was to determine why R-prime's CC evaluation failed and how to avoid similar failures in future.

* 2007: the first dead-end encountered was an attempt to unify CC and DCID 6/3 using the Single XML Description (SXD), later recast as Single Extensible Description, but this line of research and development did not pan out. It was determined to be insufficient for a contribution, technically infeasible, and overcome by events.

* 2008: direction shifted to developing a tool for improving inter-accreditor communication, for use by the developer or accreditor. Conclusion from this effort: that C&A is more complicated than DCID and CC. A digression into historical research followed, looking for commonalities; some interesting things were found.

* 2009: conclusion that no tool could possibly work until the underlying problem was better understood. Third case study (R-double-prime) found; extensive data collection followed. More blind alleys explored. At the end of the year, research at a dead-end and depression.

* 2010: Breakthrough (in January) with the insight that asymmetric information was the key to the fundamental problem. Two more blind alleys were explored and rejected. Accreditors have stopped cooperating; that line of inquiry is stalled. Risk market idea developed. Abstract model of accreditor communication developed. Link to economic theory found. Proof that a market exists was found. Abstract simulation work begun. Accreditors found to be more accepting of abstract model. Invention of risk space trajectory idea. Planned to validate the risk trajectory concept by showing that it predicts (retroactively) events in case study records. Confirmation of status viva scheduled with high

confidence of success in the new plan.

My confirmation of status viva was scheduled for 10:00 am in Oxford on 16th December 2010. The results were not what I wanted, but extremely valuable nonetheless and clearly something I can work with. The changes are going to add another ten months of work. Feedback from the assessors was clear and they want to see me back here again in less than two terms with a completely different data analysis. I intend to do exactly that.

I met with Dr Jirotka and Dr Flchais at the scheduled time. I had prepared a written agenda, not knowing the protocol for these meetings, but it went out the window immediately. The assessors were concerned from the start because the written work they received along with my confirmation report was not at all what they expected to receive. They were expecting to see completed chapters, not a presentation of interesting new results and a plan for following the new method in a new direction. The assessors were clearly upset, but we instantly agreed to shift the purpose of the meeting to a plan for getting back on track in the time available and giving the assessors what they wanted to see in the first place.

First, said the assessors, my thesis is too broad. The prediction idea and mathematical model that I have spent so much time on recently is a waste of time and should be dropped. Actually, it should be moved to future work, as the prediction result would be a valuable contribution itself, but I need to concentrate the DPhil work on deep analysis of the data I have already collected. The assessors were insistent that the data I have on three case studies is the most valuable thing in my possession---'other people would kill for it', they said---but the assessors were expecting to see a deep analysis of that data at this time, not a bunch of work on a simulation with possible future predictive value as a tool. I have been going in the wrong direction. The assessors want three new chapters to be inserted into the dissertation TOC, one for each case study, each chapter containing a methodology for how the information was collected and a 'light' grounded theory analysis. That will take three months of full-time work for each case study. I should use a tool called Atlas T-I. I should give each case study a meaningful name within the context of the dissertation and refer to them accordingly in the text. The assessors were quite insistent that the data I have collected are extremely valuable and must be analysed and published immediately. Each case study will have its own grounded theory and the overall theory is a risk market.

Why have the data not been analysed in depth? Because I was operating under the impression that the data, being participant observations, was thereby contaminated and not suitable or allowable for direct use. I thought that my more recently developed abstract model, having the potential for predictive value as a tool, was a more valuable contribution. I thought that my narrowed-down thesis, focussing solely on the predictive value of the model and having two falsifiable tests possible on it, was the way to go. The assessors redirected me onto a different path. They disliked strongly the sequence I planned of an argument based on use of case studies to validate a theory that seemed to them to have been thought up out of nothing. Admittedly, that advice rings consistent with earlier advice I had received from one of the same assessors at transfer of status time and also from Dr Martin. I had forgotten the earlier advice. What I am being told here is that a much stronger argument is constructed by beginning with a rigorous analysis of the data, then showing that the analysis points inevitably

towards the proposed solution. I protested that it felt like a rigged game. The assessors proceeded to convince me that it is not in fact at odds with the scientific method, but rather a necessary adaptation common to fields where experimentation is infeasibly expensive, such as software engineering. They convinced me. They convinced me that the data I have are extremely valuable and that the thing I need to do next is to publish a deep analysis of that data so that it becomes available to others. I did not know that I had something that valuable. The risk market idea is also valuable, said the assessors, but far more so if presented the right way as an inevitable consequence of the data analysis. The assessors gave me this advice from the perspective of those who know how examiners look at dissertations. I believe them. I will follow the advice.

The literature review also needs to be rewritten with an analytic thread going through it, leading the reader inevitably towards the conclusion that what is needed are three case studies and a risk market solution. We had an interesting philosophical discussion at this point about the way that dissertations are supposed to be written and the standard for evidence in science and in this type of research. Experimentation in software engineering, everyone agrees, is prohibitively expensive most of the time and consequently the way research results are written up in this field differs from other sciences. Rather than the sequence I had proposed (three case studies, followed by the idea of a risk market, followed by an analysis in terms of a risk market), a much cleaner way of presenting the argument is:

1. Three case studies. 2. Three analyses. 3. Risk market.

...with the risk market concept emerging as a consequence of the analysis of the data, not the other way around. Of course, this is opposite from the way things actually happened, but the dissertation is supposed to be a watertight argument and the assessors strongly recommended casting the argument in this way to avoid problems with examiners later on. This led to questions about my choice of an external examiner; I related that due to the abstruse topic of my area of research, I thought that Dr Ian Levy of CESG might be an effective---if likely to be difficult to satisfy---external examiner. But the assessors warned against it, saying that there was no point in deliberately choosing a risky external examiner, that Dr Levy---not having a university affiliation---would be difficult to justify and appoint, and that a better choice would be someone conversant with the grounded theory technique used in their suggested analysis and with security research in general, since there are no good choices available amongst experts already familiar with the topic of my dissertation. Since this is a very specialised sub-field and no one else in the world is working in it, they suggested that perhaps Angela Sasse would be a good external examiner. Regarding the evolution and presentation of arguments, advised the two assessors, I should follow the lead of mathematicians writing out their proofs: the elements of each argument are presented in the most logical order, exactly as if they were originally developed that way. In truth, of course, the process is messy, iterative, and full of mistakes, but you don't write it down that way. Omit every failure, blind alley, waste of time and error that you made; present the argument in the clearest form possible, with no extraneous detail, as if it were received from an omniscient God. Like the literature review, the reader should be led through the entire argument with the feeling that the whole thing is inevitable.

The assessors rewrote my table of contents. Besides the aforementioned literature review changes (throw out all the interesting historical information I found; anything that does not lead the reader directly

down a single analytical thread towards concluding that what is needed are three case studies and a risk market solution should be eliminated as irrelevant) and the structure of three case study chapters, the methodology must be specifically tailored to justify the conclusions to be drawn from the data in each case study. We went over a figure that appears in two of my papers, the Venn-like diagram of overlapping areas of responsibility that I found in the second case study, and we talked about ways of grounding the analysis (that the figure tries to convey) in the raw data. I proposed a method for documenting the source of each class in that diagram by reference to---for example---a particular email in the raw data, but Dr Jirotka countered with the question, 'how would the reader know that the data presented are both consistent and complete?' I responded with a variation of the proposed method that would similarly link every email in the corpus with one of those assertions---or none---and locate and highlight any inconsistencies found in the data. I am not sure how the question of deliberate hiding of inconsistent data could be answered to complete satisfaction---what I think Dr Jirotka was getting at---although Egger's Regression and funnel plots are an intriguing pair of methods I know about for doing just that with certain types of statistical data. Unfortunately these methods are inapplicable to the type of data I have. I need to talk to Dr Jirotka again to clarify her point.

The assessors said that it was clear from my relating of all the blind alleys I have explored that the risk market is a good solution. I described the suggestiveness of the validations I have tried against it: Spence's 1973 criteria for signalling and Akerlof's 1970 test for reliability both point to the existence of a market. The assessors were satisfied that the analysis is inside my head. What they wanted to see at viva time was a written analysis in the form of three new chapters.

I contacted Shamal Faily immediately after the meeting to ask him for suggested references to the grounded theory technique; he used it extensively in his own research. Shamal wrote me back with some information. Dr Martin is out of the country and I do not have Skype-compatible hardware on this laptop, so I have to communicate by email until I get back. I only have an intermittent network connection, so I am checking mail at odd times. I will get back in touch with people as soon as possible; I thought it was important to get this report written first.

Miscellaneous notes:

Coding of the three case studies will take three months of full-time work each, said Dr Flchais. Writing up will take another six months after that. I will get a copy of Atlas T-I to use for the grounded theory work. I should aim for a 'lighter' grounded theory. I need a methodology for the data analysis tailored to each case study, then I need to go through all of the data and encode meaning. The theory is important. In the methodology, I should say why I am using case studies, and why these particular case studies, but 'opportunity' is a perfectly good reason. Each case study has its own grounded theory and the overarching theory is a risk market. Just showing the problem is a useful contribution. The most valuable thing I have is the data, and an analysis of that data systematically. The numerical MATLAB model is the wrong way to do it. Issues: commonalities, case studies, and email---all the email in all three corpora.

I got the impression that in a 'future work' section of the dissertation I would be allowed to talk a bit about the risk trajectory plots that I began developing in simulation. The assessors disliked the numerical

simulation as a central part of my thesis, but said that if I nailed down more clearly the parameters and forgot about the model for now, then I could use it later. It might be better not to waste any time at present on trying to plot risk trajectories within the case studies; leave that for future work and do the grounded theory analysis. Three case studies, done in this way, would be an excellent contribution, they said. Abandon the idea of prediction---explain instead. Analyse the data systematically.

I still think that my other model, the one of inter-accreditor communication where each accreditor has a security clearance corresponding to the classification of the data on one side of the CDS and accreditors refuse to violate security policy, has value to the argument for a risk market. The assessors seemed to feel that the idea of asymmetric information and a risk market was a valid theory. They wanted it presented without any attempt at validation, however, nearer the end of the dissertation since they were unconvinced that it was a falsifiable hypothesis.

I asked the assessors for advice on handing the problem of reviewers and readers who are unfamiliar with the background of my sub-field---a chronic problem, since there are almost no specialised journals, conferences, or even more than a handful of other people working in this area. They recommended that I publish a review article in a journal. It should describe the unique qualities of CDS accreditation, mutually distrustful stakeholders---use the term 'stakeholders', they said; it has a technical meaning in grounded theory---the problems introduced by security classification and clearances, and any other required background knowledge for understanding the arguments I need to make in the dissertation. The review article ought to match the literature review, said Dr Jirotka. Review articles get cited a lot, too, which is a bonus.

I should plan to confirm again in no more than two terms with the same assessors. The assessors will talk to DGS and get me the two terms of additional time. I should not need to talk to DGS. The assessors asked me directly if I can really afford to spend the necessary amount of time to re-do all this analysis. I told them that I will do it. They asked me about funding; I reminded them that I am a self-funded graduate student and asserted that I will make it work. They noted that, since I am self-funded, there may be a bit more leeway for DGS to allow the necessary time. No funding council is putting pressure on DGS regarding my situation. If I keep my head down and make progress, I should be allowed the time.

The real gold I have is the data; I should put the numerical model aside and report back with two completed analyses (chapters) finished in hand. The new table of contents looks like:

Chapter 1: Introduction Chapter 2: Literature Survey (targeted to lead the reader inevitably to the conclusion that what is needed are three case studies and a risk market solution) Chapter 3: Methodology Chapter 4: First case study: specialised methodology for it, the data, and grounded theory analysis. Chapter 5: Second case study: specialised methodology for it, the data, and grounded theory analysis. Chapter 6: Third case study: specialised methodology for it, the data, and grounded theory analysis. Chapter 7: Interpretation: risk market theory Chapter 8: Summary and Conclusion

I emailed Dr Flchais to ask if the above matches what he had. My notes were unclear on the point.

```
Dr Flchais warned not to put important data in an appendix; examiners
do not read appendices.

Conclusion: the viva was not a complete disaster, and yielded a large
amount of specific and useful information.  I have an unanticipated and
very large amount of work to do now, beginning with learning the grounded
theory data analysis method, then applying it to three case studies.
If I follow this advice and do all of the work successfully in the time
remaining, I will finish and have an excellent dissertation that will
satisfy the examiners.

My old task list is largely irrelevant; a completely new one is needed.
I need to meet with Dr Martin as soon as possible.  The next report will
have a task list.

Joe Loughry
Doctoral student in the Computing Laboratory,
St Cross College, Oxford
```

End of WAR 0167.

I hadn't been hurt enough. I wasn't bitter enough. I am now.

References