File 20101029.0557: Weekly activity report 0160:

weekly activity report 160 (loughry)
Joe Loughry
Sent: 29 October 2010 05:57
To: Niki Trigoni; Andrew Martin; Joanna Ashbourn
Cc: 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. 20101028.1312 (GMT-7) sequence no. 0160, week 3 MT

I met with Dr Martin on Wednesday. Julie Sheppard reports that the confirmation forms still have not come back from my college to the department. We looked at my confirmation report and Dr Martin made a few suggestions for altering it to be more useful to the assessors. In general he said it was OK. The report was written from a risk management perspective, calling primary attention to the major risk as I see it, that of a late change in the research direction. Dr Martin advised that what assessors are really looking for is evidence that I am well down the new path, on track and on schedule to finish in time. In fact I am; I have spent years steeped in this problem and have dragged a pile of evidence down the new path with me. I have repeatedly tested the new approach against observations collected in the field and found that the results have not falsified my hypothesis. I have followed a number of blind alleys, enough to recognise one when I see it; this one is deeper, I have not found a dead end yet and all the tests I have done so far---a proof that Spence's criteria for signalling are satisfied, a proof that Akerlof's requirement that signals must be expensive is satisfied, and the suggestive isomorphism between the convergence behaviour of the model and observations of CT&E and ST&E negotiations in both case studies---all tests so far have succeeded and the hypothesis still holds. So I am growing confident that the theory is correct. I keep trying to disprove it but it seems robust.

I have been thinking about the kind of hard questions that might come up in the confirmation viva. In particular, how do I justify the claim I have made that convergence behaviour seen in the model has anything to do with the progress of accreditations? The gross behaviour is similar to be sure, so there is a correlation, but if the similarity is anything other than coincidental, there must be a commonality in the mechanism or a higher level cause because there certainly isn't a direct causal link.

I reported that I am confident of the convergence argument, but still a bit wary of the claim that I can predict the final configuration from three early observations of the trajectory. Because the convergence happens so slowly---accreditations sometimes take years---rather than waiting for for the orbit to decay, we predict the final outcome instead (the shape of the envelope is our risk tolerance.) If the orbit is stable, then yes the maths work out. But if it turns out to be fractally unstable, as Dr Martin noted, it may be a chaotic system. Even in that case, I claim there is an attractor that can be characterised precisely. So there are two responses to that objection, a primary and an alternate.

Dr Flchais will be sure to point out in the viva that theories must be falsifiable. I need to have an argument prepared. Dr Jirotka will have other questions.

Dr Martin suggested that the assessors might not have those sorts of questions uppermost in their minds. What they will be looking for is the

general big picture question: how do I intend to validate the theory, and how can they be convinced that I am a long way down this new path, unlikely to abandon it like others? How much of the basic work has been done? The report was purposely written concisely; an awful lot of details were left out for lack of space. I can discuss alternative interpretations, rejected hypotheses, blind alleys and evidence that I would have liked to consider but either lacked access to or did not have time to chase.

The body of the report is fine. The appendices need some polishing. The table of contents of the dissertation is a mixture of prose and bullet points; bullet points are fine but they should be cleaned up and presented in a more clear form. Also, to justify the claim that Chapters 1--3 are essentially already written, it would be good to show word counts for each section of each chapter, in lieu of simply appending whole chapters, to give the assessors a feeling of assurance without forcing them to read chapters that are still in draft form. I will go through my drafts and get the word counts, then annotate each of the section headings with that data. I will send the revised report to Dr Martin tomorrow morning and Fedex copies of the written work to Julie Sheppard before Monday.

Dr Martin requested that I explain where each of the the attached papers fit into the structure of the thesis. Right now the papers are appended without any explanation of where they fit. Of the three papers attached, one has been published, one is in draft, and one has been repeatedly rejected from conferences. I think the latter was because the editors never understood it. The idea is a controversial one. I have changed the presentation of the central idea of my thesis a few times since I started; it began as a simple failure investigation. I have concluded since that the failure of the first case study was not just a matter of certain persons being on the critical path; it was a failure of the C&A system and as such it was inevitable and would have come to the same end regardless of who was on the critical path. I have talked with several developers and accreditors about my thesis in recent days and they are much more willing to consider it in its present, more-abstract form. More conferences, I think, will be willing to publish it. It is less adversarial when presented in abstract form.

I got my passport back from the Consulate with a new visa; I am free to travel again. The biometric residence permit has not arrived yet. I require a few weeks lead time to buy tickets at the discounted rate, but I will be in Oxford at the assessors' convenience whenever they want to talk to me.

Finally we discussed what I should work on next, between improving the MATLAB model or finishing the Crosstalk paper first. Dr Martin noted that the Crosstalk paper has been hanging fire for a long time; it would be good to have it finished. The same paper also forms the latter half of Chapter 3. An excellent thing to have in your pocket at viva time, said Dr Martin, is a good answer for the assessors' question when they ask to see what you have accomplished since the written work was submitted. Having some good solid results to point to will make for a positive impression of your rate of progress.

The baseline certification and first site accreditations of Case Study No. 2 are proceeding. UCDMO acknowledged receipt of the TSABI accreditation letter and are processing the entry. The baseline list has not been updated, but is expected any day. In last week's CDTAB meeting, UCDMO made the determination to split the remaining TORAs into two groups, deciding to rule on the data link TORA first. The three initial SABI

sites were supposed to go before DSAWG in December, but none of them got their paperwork in on time. So those sites are not going to be the pushing force that the developer and PMO were hoping for to get SABI across the CDTAB threshold this month. SABI is turning into at least a 90 day process, something that is beginning to irritate the developer, Programme Office, and the service CDMOs.

The developer's installation team remain extremely busy. I had an interesting discussion with the chief engineer about an operational difficulty the developer encountered that is related to C&A. Hardware product cycles for the computers that the CDS runs on are becoming a problem again (this happened before with OS versions TSOL 2.5.1, TSOL 8, and TSOL 8 HW 4/01 and 12/02 most severely). Now it is happening again with Solaris 10 TX certified edition. The hardware vendor fails to consistently maintain its hardware refresh cycle in sync with evaluated versions of the operating system---which are the only releases that certain customers, namely defence contractors, are ever allowed to deploy. Banks and other commercial customers care less about Common Criteria certificates because they do not have a mandate to use only evaluated versions; they care much more about device driver support for the latest chipsets; the OS vendor follows. The result is a ludicrous situation in which the only hardware certified to run the highest-security evaluated OS cannot be purchased because it is out of production. The cost of the evaluated OS version is already an order of magnitude higher per licence but the only hardware it will run on is refurbished kit on eBay. Serious problems with sourcing hardware for classified installations have occurred at least three times in twelve years. The developer and Programme Office allocated additional funds and time during this round to migrate to a multi-architecture OS deployment strategy for RM 5.0; the next version (6.0) will abandon the evaluated OS for an evaluated version of SE Linux, an event directly attributable to the hardware vendor's lacklustre support for the CC evaluated versions of its operating system. The fact that Oracle sharply increased licence fees immediately after acquiring Sun Microsystems, Inc. would be, in the developer's view, a minor but reinforcing point in favour of an immediate transition to SE Linux. With the addition of auditing, functionality is equivalent; CC certificates are now available for RH and SuSE distributions including the NSA patches, and the only serious difference from the developer's perspective is the security policy definition mechanism. Nevertheless, an OS change is a recertification trigger and this is a good indication of how seriously the programme office takes the OS--hardware issue.

I finished the quarterly report for the Air Force but now I owe them a yearly summary report. The experience of running a contract research project is invaluable, but a PI sure does have to write a lot of reports. In the past two years, we have successfully achieved almost all the goals we set out to accomplish; the contract runs for one more year. I am looking forward to getting a few publications out of our results.

In this week's Security Reading Group, Shamal Faily introduced a 1985 paper by Peter Naur, called 'Programming as Theory Building' published in Microprocessing and Microprogramming, vol. 15. Dr Flchais, Dr Martin, Shamal, myself, John, Wattana, Anbang, Ronald and one other person I could not recognise on the camera image were there. Audio quality was good but the video dropped out frequently. The major case study in this paper is of two compiler-writing groups. The author is a compiler expert; Naur developed the ALGOL 60 compiler and won a Turing Award. The question posed by the paper is how theories differ from documentation and source code.

Dr Flchais noted that ‘theory’ is an interesting word for it; theories are supposed to be falsifiable. I asked whether theories can be transmitted; can they be taught, learnt, stored, retrieved, or compared? Dr Flchais was of the opinion that theories cannot be concisely written down. Shamal told a story about an apprentice jade dealer, who heard from his master endless stories about jade, telling where this or that piece of jade came from, but the master never gave any formal lessons; how did the apprentice come to learn the master’s theory?

I thought the paper was a nice philosophical walk in the park, for a change. To link the theory idea to security, consider the example of reverse engineering. I wondered aloud whether the term ‘reverse engineering’ had been coined yet in 1985; that was right around the time when a start-up called Compaq was duplicating the IBM PC BIOS by analysis of the object code and API docs. The author of the paper, in Section 6, seems to assert that it is never the case that programmers receive a system without any documentation and have to develop a theory of it. That is not true; hackers do it all the time and an attacker sometimes can develop a better theory of operation by observation of a piece of software than the designer had, as evidenced by the fact that the hacker manages to make the programme do things the designer never intended. (I completely forgot about the example of Enigma, which Dr Flchais pointed out.) There was a recent report in U.S. media: an article by Seymour Hersh in this week’s New Yorker about the Chinese government’s reverse engineering of a U.S. Navy EP-3 surveillance aeroplane captured in April 2001. They reverse-engineered the embedded operating system and probably the stream cypher key generators from surveillance and crypto apparatus that had recently undergone rapid declassification; the evidence is that it took them less than the seven years between capture of the aircraft and when disclosure came early in 2008. Someone else mentioned the Samba project as a successful example of reverse engineering, and of course there is always DeCSS.

Theories may be incorrect or incomplete. But what about purposely misleading theories? A security system designer may choose to design portions of the system in such a way as to engender false theories in the attacker’s mind; a discussion of honeypots followed. Code breakers and consumers of intelligence in WWII did something similar; they modified or controlled their own behaviour in order to give false impressions to the Axis powers of the efficacy of their own security systems and those of the attacker. It may be possible to design security systems similarly. See the article from the Guardian recently that told of how statisticians estimated WWII tank production from analysis of a fragmentary record of serial numbers obtained from captured hulls; the estimate of 256 tanks/month was within 0.5 percent of the actual value, established after the war. If the Germans had obfuscated their sequential numbering system, the British would never have been able to establish that theory.

John brought up theories developed by an Information Systems Security Officer. Are they required to be complete? No, the ISSO can made decisions with an incomplete or even incorrect theory, so long as the predictions yielded by the theory are useful. Programmers need a complete and accurate theory to make changes to source code, however. Dr Flchais asked about the impact of incorrect theories. The author makes the case that they lead to decay of the programme text. I brought up the idea of revival of dead programmes in Section 6; all this talk of incorrect theories suggests that storage and retrieval, in particular the ability to checkpoint theories would be a fruitful line of research and development. Shamal mentioned knowledge management systems in that regard. Can theories be compared? If so, they could be improved, distributed, and debugged.

I mentioned a paper from an unrelated discipline, Yuri Lazebnik's unusual paper from cancer biology, 'Can a Biologist Fix a Radio' (Biochemistry Moscow 69(12), pp. 1403--1406, 2004). That paper is all about theory building. It is odd that none of the references overlap with Naur's paper on a similar topic published twenty years earlier. Lazebnik talks about incorrect theories, why incorrect theories are sometimes useful, and how theories are improved. The way biologists develop theories is totally different from computer programmers, but they way they use them is just the same.

Other reading this week: on the topic of signalling theory, in hopes of finding a more solid justification for some of my claims, I have been reading about situations where signalling breaks down (one example is credential inflation). Evolutionary biology originated the concept of signals; economists adapted it from there. There is a subtle difference between 'signals' and 'cues' (with a distinction assigned to 'honest' signals) that I think I can use. An animal may send honest signals to a predator that directly and understandably benefit both the animal and the predator. That is a very interesting idea which I think has application in the domesticated covert channel that I am investigating. I may need to extend my background reading in another unanticipated direction.

My current task list (in priority order, most urgent first; work on tasks in this order):

1. Make the requested changes to confirmation report. Fedex n copies of all written work to Julie Sheppard tomorrow.

2. Write an FY2010 summary progress report for the Air Force for probabilistic redaction project.

3. I believe I should prioritise the Crosstalk article next, as that equals a good chunk of Chapter 3.

4. MATLAB progress has been languishing. What is needed is a generalisation or overlay of more than one simultaneous simulation with the same set of fixed points. Implement Prof. Polak's equilibrium acid test and the double alarm clock option model at the same time.

5. Background reading: Pennock and Wellman (2004) on uncertainty markets, Levitt and Dubner (2009) on asymmetric information, Bernstein (1996) on risk assessment.

6. Ping the following people: Paul Ozura, Dennis Bowden, Patti Spicer, Charles Nightingale, Hal Forsberg.

7. Coordinate with Colin Murphy re: OUSS (first thing in the morning before the next lecture).

8. Small tasks: update first case study chart with changes from last conference; draw fault-tree diagrams for R-prime, R-double-prime and S-star; draw up organisation charts for R, R-prime, S-star, R-double-prime, N, L and G; update documentation of the current set of anonymisation codes.

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

End of WAR 0160.

References