File 20101008.0532: Weekly activity report 0157:

weekly activity report 157 (loughry)
Joe Loughry
Sent: 08 October 2010 05:52
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. 20101007.1349 (GMT+1) sequence no. 0157, noughth week MT

I met with Dr Martin on Wednesday. I familiarised him with some
of the results I have found from simulating economic interactions of
accreditors by means of a physics-based model implemented in MATLAB and
by validating the MATLAB model with a real embodiment. The physical
model that I built (screen door springs nailed to a board) immediately
showed up some interesting and unexpected behaviours that are, of
course, implicit in the MATLAB model but only show up when the time
scale is cranked down to microseconds. For example, when I pull the
pin to release the model from its starting position, the real model
orbits the final position for a while before settling down to rest.
I am wondering if I should look for an interpretation of that behaviour
in terms of accreditor--accreditor interactions, or whether it is merely
an artefact of the physical world that ought to be ignored. I am leaning
towards believing it is significant (see below). Other aspects of the
model that I still have to figure out include the accreditors' position
along a continuum of risk tolerance, how to measure an accreditor's
'pulling power' (what I am calling influence) on other accreditors'
positions and on risk moving around the game surface, and whether an
accreditor's influence is affected by the accreditor's reputation.
An accreditor's reputation amongst other accreditors and data owners
is affected by the accreditor's mistakes. An accreditor's reputation
with operational sites and with CDS vendors or installers is affected
by that accreditor's success at accrediting operational installations.
Reputation affects influence in my abstract model. Influence is the
analogue of the spring constant. I think influence remains constant
over the lifetime of the model.

Also with respect to the model, the damping or friction coefficient
is currently a mystery. What does it correspond to? Clearly it is
necessary, because otherwise the system will never settle down, preferring
a dynamic metastability. It occurs to me that perhaps metastability is
a more faithful model of real-world accreditations than a fixed point
would be. Dr Martin was the first to suggest metastability to me. I had
been concentrating on what I believe to be a theorem: that a fully damped
system will always settle down to a unique fixed point---I need to talk
to a physicist about this---but I cannot cite a theorem at present to
prove it. I think it relates to the fact that there is no energy input
to the system, and damping converts the kinetic energy of the system to
thermal energy, so it must converge to a minimum-energy state. Instead,
I now want to borrow a technique from dynamical systems, called a phase
space plot, and show that the dynamic metastability of my system converges
on a stable attractor orbiting around the ideal (minimum-energy) ground
state of an optimised residual risk accreditation. I think this will help
in the post-accreditation (rating maintenance) phase. It feels right.

I asked Dr Martin for advice on how I should handle two related issues
in the confirmation report: the fact that my economic interpretation is
a recent discovery, and the fact that it was actually a reaction to the
difficulty I have had getting US and UK accreditors to talk to me. Dr

Jirotka, in my transfer viva, encouraged me to do an ethnomethodological study of those accreditors, but when I ran into more and more difficulty getting the data, in the interest of time I decided to activate Plan B. I made a numerical simulation that I could run experiments on. I think that was the right course of action under the circumstances, but I expect to have some explaining to do when I tell Dr Jirotka about it. Dr Martin said there is a school of thought that blind alleys are an important part of science, but people do not really want to read about them. He suggested to put in a hook in the report indicating a change of direction, but not to analyse it in too much detail. Regarding length of the report, five pages is more of a guideline than anything; if the report is ten pages long that will not upset anyone. I should try to show progress as if it were an idealised march towards a finished product, the way mathematical proofs are always written. Every mathematician knows that the process of getting to a real proof is full of blind alleys. The final proof, however, shows only the best and most direct route to the top.

The confirmation report is being written from a risk-management perspective. I can think of a lot of of risks, but I fear making the dissertation appear completely untenable. Every risk shown will have a mitigation plan attached. But I would like to show these recent developments as an example of showing adaptability. I think I can argue successfully with Dr Jirotka that the economic model is a sufficiently interesting and powerful substitute for accreditor interviews. The biggest risk of pushing too hard at the present time to get accreditor interviews is that I could burn relationships that will be necessary in future for the remainder of the ongoing research programme.

I reported that RM 5.0 received its TSABI accreditation letter yesterday, and on the minor panic that resulted when the developer misread the meaning of some words in the letter and feared that it meant something different. After I explained to them the source of the words (from Chapter 3 of DCID 6/3, reflecting the old-school experience of the accreditor as well as the newness of the NIST SP 800-53 criteria), everybody calmed down.

I asked about chapters, and Dr Martin said it is a very positive sign to see draft chapters, or at least a Table of Contents of the dissertation with some idea of what goes in each chapter, at confirmation time. I will write some chapters and TOC, after I finish the confirmation report.

My plan now is to finish the confirmation report, get it to Dr Martin, and once he has given approval, to file the confirmation paperwork and choose a date. Today, I have to finish the DARPA proposal for Lockheed, as that is my next two years of funding, and I cannot forget about the COMLAB-CS-2010 reviews that I am responsible for. I have to get my UK visa application posted this week too. I am not getting enough sleep.

Security Reading Group restarted for the term this week. John Lyle introduced a presentation on Webinos (Steglich, 2010) to a larger discussion about web OS platforms, security of personal information, APIs and deployment. Several people brought up the problem of APIs for things like accessing GPS, accelerometers, and personal address books. We kept coming back to the example of Java as a write-once/run-anywhere platform, of course; I noted the existence of Facebook games as an existence proof for the spread of an unanticipated application atop a widespread platform. I asked whether webinos could be distributed outside of the phone OS vendors in such a way that end users of phones could choose to install it as a third-party application, possibly then resulting in a community of webinos users that would be independent of

phone OS makers. Dr Martin made the point that phone makers have a time horizon of a year at most. Webinos is intended for use also in cars for satnav and entertainment systems. There is a good use case for air passengers to be able to start watching a movie in the departure lounge, then pick it up at their seat on the plane without interruption.

Dr Martin and John Lyle are away next week. Shamal asked if anyone is going to ACSAC, and we talked about some of the classic papers that have appeared in that conference. I wish I could go, but I have no time to go to that conference. I am aiming for the 10th Workshop on the Economics of Information Security (WEIS) with my next paper.

I have a new MATLAB book (Harper, 2007) on solving dynamics problems. I hope to have the MATLAB simulation more closely matching the behaviour of the physical model soon, with phase space plots showing a stable attractor decaying to a fixed point.

RM 5.0 received its TSABI accreditation letter, satisfying the requirement of at least one ATO in the BOE for UCDMO Baseline listing, although the accreditation letter is not the ATO; that comes from the recommended in the DNI Test Director's final report (DNI, 2010). The UCDMO CD Baseline is published nominally once a month; October has not been released but the developer expects RM 5.0 without follow-on capabilities to appear. The wording of the accreditation letter (Dister, 2010) caused some consternation in the developer's organisation because the letter used the obsolete language of DCID 6/3 chapter 3 instead of that in the NIST SP 800-37/53 criteria: the phrase '...with a High Level of Concern (LOC) for Confidentiality and Integrity and a Medium LOC for Availability...' means that the CDS protects these things well, not that the accreditor has concerns about the functionality. After I explained the meaning of the language to them, the Programme Manager and PMO stopped panicking.

There was no meeting of the CT&E telecon this week; there will be no more weekly telecons unless something new goes wrong. The September 21--22 CDTAB examined the RM 5.0 architecture in detail; additional TORAs in October will examine various follow-on capabilities. Three or four customers are going to CDTAB and DSAWG for SABI approvals soon. There will be two accreditation letters (it was supposed to be a unified process by now, but there will be two letters, one for TSABI and one for SABI). Orville Brown managed to get the TSABI letter out of DNI this week. The developer feels that 'everyone is afraid to step on any NSA toes, but NSA is in no hurry. Every time someone says ''do not put them [RM 5.0] on the list'', they are overruled by someone else.'

Reviews for the COMLAB-CS-2010 conference are beginning to come in; I got one good review of my submission titled 'An Artificial Risk Market Solution to the Problem of Information Asymmetry in Cross Domain Systems Security Test and Evaluation (Extended Abstract)' although I expect it to be left out of the conference programme since we have far more submissions than space. Any reviews are valuable, though, to improve my paper before the next conference. I owe them seven reviews, due 13th October; I will try to get them written and submitted over the weekend.

I wrote a response to DARPA RFI SN-10-73 ('New Technologies to Support Declassification') for Lockheed requesting funding to work on an interactive declassification tool---a type of cross domain system. I proposed an interesting reverse application of map-reduce for it that should greatly improve the quality control of the resulting system.

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

1. Confirmation report is past due to Dr Martin.

2. Update the Oxford University Scientific Society web site and term card (tomorrow).

3. COMLAB-CS-2010 reviews (this weekend)

4. Email Dennis Bowden with my standard set of questions.

5. Finish the Pennock and Wellman (2004) tutorial on uncertainty markets (Friday).

6. Submit forms for confirmation of status to Julie.

7. Get a date set for telecon with Patti Spicer, Charles Nightingale and Hal Forsberg at CSC.

8. Quarterly progress report and FY 2010 summary progress report for the Air Force

9. Implement an option mechanism based on the Dutch pattern; implement 'acid test' as unit test.

10. Appendices A--D of the confirmation report.

11. Small tasks: update first case study chart with audience suggestions from VALID 2010 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.

12. Got a reply back from Paul Ozura; he was on holiday and asked for a bit more time to respond.

13. Crosstalk article: immediately after writing confirmation report, write the interpretation of the first case study in terms of accreditor behaviour incentives; write a preliminary overview of second case study based on final reports from NSA I173 and I733, DNI CAT, ST&E, POA&M Validation Report, and CDTAB.

14. Based on what I learn from Paul Ozura, rework the other two planned surveys done for background on the case studies.

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

End of WAR 0157.

References