File 20100702.0520: Weekly activity report 0143:

weekly activity report 143 (loughry)
Joe Loughry
Sent: 02 July 2010 05:20
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
Attachments:
Weekly activity report no. 20100701.1403 (GMT-7) sequence no. 0143, week 8+2 TT

I have begun getting things off my task list and done. New things have been added, so it is no shorter, but some old items are beginning to disappear.

Reading Group met on Monday to discuss Shamal's paper on security Chindgu, after Prof. Sean W. Smith's seminar on TPM and virtualisation in OpenSolaris. Cornelius opened a Skype channel to Room 478 for me. Prof. Smith is a good speaker; throughout his talk I kept noting techniques I want to remember for when I give talks in future. The time pressure commonly felt by PhD students in the UK makes it difficult to learn everything in three years---in addition to adequately exploring a topic for a good dissertation---starting from scratch. Students, of course, lack experience of their own to build on, so it takes longer for them to integrate the entire body of existing work; more experienced researchers need less time to apprehend a sub-field before getting to the point where they can make a substantive contribution. In some of my reading last week and discussions with Dr Martin, I was trying to get at those characteristics common to students who finish on time. I met with Dr Martin on the 25th to check in and update progress. I described some of the interesting rabbit holes I explored this week, in particular the idea that researchers like Everett Crosby formalised in 1905 about the way people acquire and communicate information about the level of risk in asymmetric information environments. Akerlof's (1970) paper on 'Quality Uncertainty and the Market Mechanism' defined two channels by which people communicate information about unknown quantities ('quality' in Akerlof's scenario, risk and risk mitigations in the variant way I want to apply it); he also talked about the cost of dishonesty, which I believe may apply to the turf wars that occur in CDS accreditation. Turf wars take the form of limiting information, not the provision of incorrect information, but I think the connection may be there nevertheless. I am trying to adapt Akerlof's mathematical model; currently I am busy trying to map the concepts sufficiently to get a simple statement of fact to make sense numerically. The market idea in my ACM CCS workshop paper is only half-baked; I have been thinking hard on how to get it operational in time for the conference deadline. I decided that the paper I was planning to submit on the 28th was incomplete without a demonstration of the model; on the due date I emailed to ask the conference editor for an extension and was given until 9th July. If I can make Akerlof's formulae fit the players in my scenario during the next couple of days (by Sunday), I should be able to finish the paper. If not, then the idea did not work and will have to be abandoned for lack of time. I hope to present the paper to Reading Group on 14th July before the summer break; John has got next week.

This week I spent more time than I wanted to spend on Lockheed work. I am behind schedule on two work assignments and at least that much work on my thesis. The RM 5.0 certification telecon that was supposed to occur today was postponed to 8th July, but I talked with people who were at Ft Meade and SSC Charleston for the lab installations. Beta 2 starts officially next week. Installation in two labs for government regression testing of the latest build is done. The current build (not 5.0zc) is the one that will be certified according to the Project Manager; this build contains all approved CRs resulting from Beta 1 findings. There might be one new issue that could trigger a new build: it was being tested yesterday but I have not heard the resolution. STRATCOM opeval begins in two weeks, following ten working days of government regression testing. The developer related that many of the findings out of Beta 1 were political in nature, but developer representatives were able to work out the concerns of the testers. Interestingly, SSC Charleston testers are said have a different personality from those at Ft Meade---the Ft Meade testers were much nicer. Charleston, it was said, raises a fuss every time they find the slightest deviation; for example, some system administration tools that were left on the test machine for the purpose of facilitating reconfiguration of network settings during testing. It was done that way on purpose for the convenience of the testers, but the testers in Charleston declared that they would write up every one of the files as a finding anyway (going by the book). In response, the developer's Test Director, Mr Phillips, will make sure to lock down the Charleston machines especially well next time, just to make the Charleston testers' life difficult. The testers got precisely what they asked for: their life made difficult. Developer--certifier interactions continue to provide interesting data; this was not an example of an accreditor-squared turf war, but interesting nonetheless. Another anecdote this week provided a countering perspective---or perhaps it was related after all, in light of the geographical differences---Emily at NSA said that RM is the only CDS that meets all of their deadlines. If the RM developer says they will deliver something by a certain date, they do. None of the other guards does that, she said.

I provided an analysis to my manager at Lockheed on the impact of DOD 8570.01 deadlines for full compliance with ISO 17024 in December 2010. After re-reading the April 2010 revision of the Instruction, it is clear to me that that CDS developers will have to be certified at Information Assurance Workforce System Architect and Engineer (IASAE) Level II or Level III, not the lower IA Technical Workforce (IAT) level. This reading is based on Chapter 10 of DoD 8570.01-M in which it states that software development intended for use outside the developer's own Computing Environment (CE) at Protection Level (PL) 1 or PL-2 requires IASAE Level II, and that IASAE Level III is required for PL-3, 4, or 5 in the CE or Network Environment (NE). That clearly describes a CDS. I was at least able to reassure the manager that IASAE is not mandated until calendar year 2011. This is going to affect all CDS developers. It should improve assurance for CDS systems (at least, it imposes new requirements), but at present there is a shortage of IASAE-qualified personnel (there are approximately 1200 in the US). Which brings up another question I want to ask in my DAA surveys: how willing are DAAs going to be to give out 180-day waivers for IASAE Level II and Level III to CDS developers if uptake in 8570 lags? The cost, I estimate, will be at least 4500 per developer (salary plus training plus exam). That is almost the fully burdened annual cost of one software developer for the size of a typical CDS programme.

Dr Martin and I talked on Friday about my thesis and the viva. As my supervisor, he said he does not have a clear idea of what the unifying theme of my thesis is. He said he thinks I have it in my head, though. I promised to write it down: the 'elevator pitch'. I have been struggling to express this clearly in the ACM workshop paper, but I will have it soon. There are two schools of thought on what the PhD is. One says that the goal is to become the world's foremost expert on your topic. The other says that it is a process of showing you are a competent researcher who can select, chase down, and finish a research project, to a defined standard of quality, in a particular amount of time. In other words, to show that you can work as a researcher. Andy Cooper once gave me advice that the key to a PhD is to narrow your topic so far down that you can document every last detail, leaving no loose threads. Dr Martin advised that the purpose of confirmation is to point to having completed the substantive contribution and now all that remains is to write up. I intend to reach that place during the summer. If I can just get Akerlof's mathematical model modified to fit my problem, and show that it works for a few test cases, then I will be able to have that much of my thesis peer-reviewed by other workshop participants. After that, it is only a matter of gathering up everything else and arranging it for presentation to the assessors.

Cornelius asked me this week for information about Common Criteria protection profiles and the threat models they describe. I sent him back some thoughts on protection profiles that I have read (those applicable to CDSs) and recommended that he look at published Security Target (ST) and Certification Report (CR) pairs instead. STs have the advantage of being tested, and are almost always published in combination with the corresponding certification report. Sometimes you can see evidence of the negotiation that always occurs between developer and validator during the validation process, before the ST and the TOE go before the evaluator. A good validator will assist the developer in limiting the threat model to an evaluatable configuration. In my experience, when I wrote a PP and two STs, the feedback I got from the evaluator (NSA) was that it was the best they had ever seen---also the longest---and it was completely un-evaluatable because it was far too long. My most recent ST had nearly the same problem. The threat model I described was comprehensive, but the amount of evaluator effort needed to test it exceeded the reasonable capacity of the national scheme. It would have made for a more useful certification to end-users because of that level of detail, but in the end it was never evaluated. I hope to have more discussions with Cornelius on this topic in future.

I have some Lockheed tasks that I have to finish next week in addition to the ACM CCS workshop paper. I owe a quarterly progress report to the Air Force about the Probabilistic Redaction project. NIST released the final Special Publication 800-53A, rev. 1 last week, and I have to compare it to ISO 27002. I volunteered to help with the Comlab DPhil student conference again this year; the committee will have its first meeting next week. I have been reading the 2009 book by Eugenie S. Reich on the Jan Hendrick Schn scandal at Bell Labs in 2002. That fraud led to the retraction of eight papers from Science, six from Physical Review, and seven from Nature. I started reading it when I felt my ideas in the ACM CCS workshop paper were half-baked. The book contains a lot of examples of unsupportable evidence in scientific papers, and can be read as a guidebook for how to do things right. What I was looking for was a standard of proof needed in a good article---obviously in relation to my proposed model of accreditor--accreditor communication during ST&E of a CDS. For others to be able to replicate it, what level of detail should I provide? I learnt something new: Robert Boyle (whose laboratory along High Street is commemorated in Oxford) was the first to say that scientists should write, with enough detail that other researchers could replicate their results, and that failures should be published along with successes.

Tasks (in priority order, most urgent first):

To be done immediately:

1. ACM workshop paper due 9th July containing modified Akerlof model. 2. Still waiting on invitation to get into CDTAB; may be combined with DSAWG and UCDMO trip (early August). 3. List of questions for the accreditor survey (including new questions added this week). 4. Get the other two surveys done. 5. Finish methodology chapter (waiting on final survey questions). 6. Crosstalk journal paper. 7. Prepare talk for VALID 2010 and submit to PIRA for approval. 8. Compare NIST SP 800-53A to ISO 27002.

To be done as soon as possible:

9. Update dissertation Table of Contents. 10. For Chapter 3 or 4, start writing the interpretation of the first case study results and second case study preliminary results. (This will be needed for both confirmation of status and for answering likely audience questions in France.) 11. Begin writing progress report. 12. Update the schedule. 13. Apply for confirmation of status.

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

End of WAR 0143.

References