File 20100604.0420: Weekly activity report 0139:

weekly activity report 139 (loughry)
Joe Loughry
Sent: 04 June 2010 04:20
To: Niki Trigoni; Andrew Martin; Joanna Ashbourn
Cc: otaschner@aol.com; anniecruz13@gmail.com; andrea@hpwtdogmom.org;
chip.w.auten@lmco.com; diane@dldrncs.com; Joe Loughry; mmcauliffesl@comcast.net;
tom.a.marso@lmco.com
Attachments:
Weekly activity report no. 20100603.0652 (GMT-7) sequence no. 0139, week 6 TT

I met with Dr Martin on Thursday morning. I reported progress on the accreditor survey. I have been in contact by email with Mr Paul Ozura and another person who is a Common Criteria evaluator, asking questions about how government accreditors come to decisions and specifically how the question of multiple responsibility is settled in CDS accreditations.

Last Friday I had a horrible thought that I might have missed something and consequently had been going down the wrong road for some time. I checked the relevant government standards (DCID 6/3, NIST SP 800-37/53) but the answer was not in there; the only way to establish the truth was to ask working accreditors. I immediately contacted a few people I knew with a set of specific questions. The answers have not come back yet; I expect to have an answer tomorrow. Fortunately, in discussing the problem with someone else later that weekend, I realised how to fix it and that the problem may not in fact be a problem at all. The model of CDS ST&E that I have developed is sufficiently general to handle both cases, and the one I thought was a serious problem is actually a subset of the other. Specifically, it has to do with one detail of the way US government accreditations actually work in practice. Looked at in the right way, it does not violate my original assumption. Instead, it is only a special case of the more general situation that exists to handle cross-national ST&E of CDS accreditations. The model is still sound.

Nevertheless, I was emailing accreditors at 1:00 in the morning with some very pointed questions. Their answers will serve as a useful cross-check and validation of a fundamental principle underlying my theoretical model. I can use the survey now to validate my original assumptions with respect to not only the US, but also UK and other Common Criteria countries also. I need to broaden my thesis a tad, closer to where it was when I started, because I can see now that it applies not just to US-only CDS accreditations but also quite neatly to US--UK accreditations as well. It pulls the CC back into the mix, but that's all right, it ties in with my first case study. US--UK accreditations assuredly would involve multiple accreditors, as would in fact any cross-national CDS installation, of which there are many in a flexible coalition environment. My theoretical model handles it fine because there are more degrees of freedom than would typically be encountered in a real situation.

This, together with last week's insight into a potential solution to the accreditor communication problem finally provided the last bit of momentum necessary to finish the accreditor survey questions. A prototype of the questions is now out in the field in the form of those emails. Before spamming the entire list with a SurveyMonkey layout, I intend to polish the questions with the help of my contacts. One benefit from last week's horrible thought panic episode was that it suggested a few more important questions that I did not realise were needed before. I am going through the on-line survey provider's user manual now. This week I finally got the attendees list for a meeting of security accreditors that took place a few months ago; the list contains names

and email addresses that I needed. The number of prospective survey participants is currently holding at 23, before the addition of this new list. I have a contact with Mr Paul Livingston, recently retired Chair of the Defence and Intelligence Community Security Accreditation Working Group (DSAWG), whom I met a few times before at DSAWG meetings.

Dr Martin asked about record keeping during these interviews. I reported that all interactions so far have taken place via email, where I have copies of all messages sent and received with time stamps. All of my written notes are copied into this file which is effectively an electronic laboratory notebook, and backed up with the rest of my thesis files. I keep a separate written log of events throughout the day with periodic time stamps; these logs are archived and I can refer back easily several years to find out what I was doing on a particular day with a time resolution of a few hours.

Next, Dr Martin and I went over my list of prioritised tasks. The accreditor survey, as promised last week, is finally under way. The application for my UK student visa needs to be done this week. I am still thinking about the market solution to the inter-accreditor communication problem; I have to finish convincing myself that it might work before I can persuade anyone else of that. Abstracts are due this week to the ACM workshop; all they need is an abstract so I am going to submit the idea. If a jury of peer reviewers does not find fault with it, that will be a good indication of potential validity. On Monday there is scheduled a two-hour classified telecon with the 5.0 certifiers who want to talk about some concerns they have. I will be at the Deer Creek Facility to listen in on that call.

The state of my to-do list is interesting to compare to what it looked like a year ago. Some items, like writing the Crosstalk journal article, are still there. Much progress has been made, though, in narrowing down my thesis since that time and focussing. The theoretical model is completely new and never appeared on the task list, and the delay in the surveys benefited from waiting until I knew the right questions to ask. Dr Martin is correct about the methodology chapter remaining on that list for so long, unfinished. As soon as I get two more papers written and submitted to ACM and Crosstalk, I will knock some of the old items off the list.

Other activities this week: the Beta 2 phase certification target executable of RM version 5.0ZC was built last week for UltraSPARC III and X64 architectures; the Plan of Actions and Milestones (POAM) for installation at STRATCOM is to be discussed Monday. Start of Beta 2 testing is still on schedule as of today. I am thinking that the Crosstalk article should include a description of Beta 2 testing and certification of RM 5.0 as a counterpoint to the Common Criteria case study, if certification is in fact achieved by 20th August. It would make the article more timely for the people who read that journal.

I have been reading an old book by Dequasie (1991) about working on a secret government programme in the 1950s, and how classification of information was handled at the time. It is a memoir and tells part of the same story as another book I read before (Clark, 1972) that was written from a different perspective. I was able to find a copy at the University of Denver library. The book contains a good discussion on pp. 182--190 of the organisation of classification hierarchies.

Lockheed has an internal system designed to solicit ‘crazy’ ideas that might turn into practical technologies one day. I submitted an idea this week for detection of paraphrased concepts by an automated

declassification tool: using a database like LDC2007T22, ‘2001 Annotated Enron Email Data Set’ to teach a machine learning algorithm to recognise paraphrased concepts from a large collection of different writings about the same topic. The Linguistics Data Consortium of the University of Pennsylvania has a catalogue of such databases including newspaper articles annotated with topic descriptors; the Enron email database is interesting from a security perspective because participants were often deliberately paraphrasing their language in email when talking about illegal activities.

Dr Martin is teaching, so our next meeting is postponed for a week.

My current list of tasks in priority order, most urgent priority first:

To be done immediately:

1. Accreditor survey new questions. List of email addresses for known accreditors. 2. UK student visa application due. 3. Register abstract for the ACM workshop in October. 4. Write up an explanation of the accreditor optimisation strategy. 5. Go through list of attendees for accreditor email addresses. 6. Classified telecon re: 5.0 certification POAM on Monday. 7. List of email addresses for the other two surveys 8. Finish methodology chapter (waiting on survey design). 9. Outline the Crosstalk journal paper.

To be done as soon as possible:

10. Update dissertation Table of Contents. 11. For Chapter 3 or 4, start writing the interpretation of first case study results and second case study preliminary results. (This will be needed for confirmation of status.) 12. Document codes in a new appendix for de-anonymisation information for all participants. 13. Begin writing progress report for confirmation of status. 14. Update the schedule. 15. Apply for confirmation of status---I want to submit the forms with written work by end of June for August or September.

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

End of WAR 0139.

References