File 20100507.0749: Weekly activity report 0135:

weekly activity report 135 (loughry)
Joe Loughry
Sent: 07 May 2010 07:49
To: Niki Trigoni; Andrew Martin; Joanna Ashbourn
Cc: otaschner@aol.com; andrea@hpwtdogmom.org; chip.w.auten@lmco.com; diane@dldrncs.com;
Joe Loughry; mmcauliffesl@comcast.net
Attachments:
Weekly activity report no. 20100506.2231 (GMT-7) sequence no. 0135, week 2 TT

I met with Dr Martin on Thursday this week. With the reviewer comments from the VALID 2010 paper in hand, I asked for advice on how to respond to some of their comments. The introduction needs be rewritten, but Dr Martin cautioned me of the need to avoid the trap of rewriting the entire thing. Generating new material is more important than endlessly revising old. Adding a whole lot of new material to the introduction of this paper is going to be difficult without busting the page limit. I should expand acronyms and abbreviations in the abstract if participants at this conference might not be familiar with them. Some reviewer comments can be left un-addressed, but this might cause a reviewer to ask pointed questions after your talk.

One reviewer did not like the formatting of Table I and referred me to the IEEE template guidelines. I did follow the template, but I will check on the table format and see if there is a more compact form. Two reviewers disliked the term ’case studies’ and suggested ’examples’ instead; sub-fields have their own preferred language and it’s a good idea to conform. Two reviewers want the introduction section rewritten to better explain the flow of ideas through the paper. The first reviewer wants a reference for the anonymised project described in the first case study; I think the reviewer’s question may be related to the need for a better introduction to explain the flow of the paper---I can’t very well reference a report on the anonymised project, that’s the whole point of anonymising it. The third reviewer was harsh: ’Although this paper has been send [sic] as a "work in progress" contribution, no work in progress is being described!!’ The review goes on to complain that after a good build-up to section IV, the reviewer was disappointed not to find a solution. I will try to respond to this reviewer with some ideas I have developed since the paper was submitted. The main difficulty is the page limit. Because I am working in a narrow sub-field, I have to explain a lot of background to non-specialists at this conference first. That leaves not a lot of room for content in four pages, even given the fairly dense IEEE format. If I can’t fully address this reviewer’s concerns in the revised paper, I will try to do so in my conference talk. I have not been notified of how much time speakers will be given, other than a request for 10 to 14 slides ideally.

The third reviewer said ’This is a great study subject’ and that the results are well publishable, but then went on to say the paper tries to make too many points. The reviewer gave me a list of specific things to look at, including some concrete suggestions for improving the introduction. I shall work hard to satisfy this reviewer.

The fifth reviewer simply summarised the paper.

The conference chairman wants to see a revised version; I will send that in as soon as possible. I updated the comlab wiki to sign up for a Security Reading Group session in a couple of weeks where I can present the paper and conference slides. Next week there is no Reading Group meeting due to unavailability of most everyone, but I will introduce my paper to the Security Reading Group on 19th May.

My trip to Nice in August is going to cost a minimum of $2,500.00. I will ask my college and the department regarding any funding support they might offer. Dr Martin and I discussed how to get to the conference; it may be less expensive to fly through Heathrow instead of Frankfurt, and the train system in France is second to none, but it might not be any cheaper. I am going to check tomorrow with Lockheed's corporate travel agency to compare prices. Because of the dates of the conference, I need to get travel reservations made soon. I will stay at the conference hotel, as recommended by the organisers.

Next, Dr Martin and I went over my task list and he helped me prioritise some items. In priority order, I should finish the travel reservations first, followed by reviewer comments on the VALID 2010 paper, the long-delayed survey questions, Crosstalk paper, UCDMO conference paper, ACM workshop paper, and the methodology chapter, followed by lower priority items. I had to leave the Skype video call by 0720 in order to drive to Lockheed's Deer Creek facility in time for a classified telecon at 0800. The last thing we discussed was co-authoring the journal article for Crosstalk. I think, based on analysing the author lists of papers appearing in that journal for the past five years, I have a slim chance of getting this planned article accepted without a high-powered co-author. Dr Martin agreed to help. I appreciate how busy he is and I will try to take up as little extra of that time as possible. I am also thinking about submitting a paper to the Second ACM Workshop on Assurable & Usable Security Configuration (SafeConfig) in October. The deadline for abstracts is 7th June. This is my Plan B in case either the UCDMO conference or the journal Crosstalk reject my contributions.

The conference call at Lockheed immediately following was with the Programme Office (government sponsor), IV&V test lead, NSA I173 and I733, and the software developer. I made it to Deer Creek in time for the start of the meeting; it was a classified meeting so I could not take notes and cannot talk about specifics. The meeting was to discuss the preliminary copy of the formal CT&E test reports for Radiant Mercury 5.0. Beta 1 is now complete. Overall, three formal testing reports will be delivered: NSA I173, NSA I733, and DNI CAP. Final versions of the I173 and I733 reports will be issued a week from next Friday, 14th May. The developer is currently writing a formal response to all findings. Details of findings are classified. All I can say is that the schedule is unchanged, with no alteration expected to the 20th August final certification date.

From the perspective of my research, however, there was one interesting detail I want to make note of: the penetration testers expressed considerable annoyance with two particular flows that the developer provided for CT&E testing but which were not fully vetted. The testers said they really had to rush to get everything tested, but then the developer responded to their final report with, 'Oh, those two flows were fake, not real ones.' The testers expended a significant amount of time on those two flows, but now the results of those tests are disregarded because the developer claims that the flows were not fully vetted. The developer countered that the [unspecified features] being exercised by [unspecified flows] were an important new feature and there are no accredited examples of it yet, so it was better that the functionality be tested than not tested. The interpersonal dynamic observed during this morning's telecon---including not just the software developers but the programme office, penetration testers, IV&V contractors, and certifier---could be an important piece of data which is why I am documenting it. Not sure where I will include it when I get to writing up later, but I think it's important.

Miscellaneous other information: results came out this week showing the number of viewers of the weekly multicast talks given across Lockheed sites. My last two talks came in 2nd and 4th place in terms of number of participants on Live Meeting and multicast, out of 22 lectures given so far this year. I had 306 total listeners on 9th and 20th April. The most popular talk was by Andy Miller on the Common Weakness Enumerations (CWE 25) on 23rd February.

I got an email from Julie Sheppard today reminding me to apply for Confirmation of Status in Michaelmas term. I plan to submit the paperwork and written work earlier, hopefully to confirm at the start of Michaelmas rather than nearer the end of the year.

Dr Martin is teaching next week but offered to meet in the evening if I need to; we will coordinate the next meeting together by email. I have to work on a lot of different things before our next meeting.

Current list of tasks in priority order, most urgent priority first:

Immediately:

1. Make travel reservations for Nice.
2. Address reviewer comments from paper and send updated copy back to Prof. Dini.
3. Go through final presentations from RMUG for names, dates, addresses, and data relevant to thesis.
4. Finish list of email addresses for practitioner survey, participant survey, and user survey; develop questions, enter in SurveyMonkey and test. Goal is now 10th May.
5. Re-outline the Crosstalk journal paper based on what was learnt in RMUG and 5.0 CT&E Beta 1 IV&V and pen testing; extend the outline; write draft paper; submit to journal by 14th May.
6. Write the rest of the UCDMO conference paper.
7. Begin outline for new ACM conference paper; write abstract.
8. Extend the outline of the methodology chapter.

As soon as possible:

9. Update dissertation Table of Contents.
10. For Chapter 3 or 4, start writing interpretation of first case study results. (This will be needed for confirmation of status.)
11. Begin writing progress report for confirmation of status.
12. Fill out paperwork for UK student visa extension for June deadline.
13. Update the schedule.
14. Design of accreditor information coordination tool based on feedback from first three papers.
15. Apply for confirmation of status---I want to submit the forms with written work in June for August or September.

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

End of WAR 0135.

References