File 20100219.1627: Weekly activity report 0124:

weekly activity report 124 (loughry)
Joe Loughry
Sent: 19 February 2010 16:27
To: Niki.Trigoni@comlab.ox.ac.uk; Andrew Martin; Joanna Ashbourn
Cc: andrea@hpwtdogmom.org; Joe Loughry; mmcauliffesl@comcast.net
Attachments:
Weekly activity report no. 20100219.1245 (GMT) sequence no. 0124, week 5 HT

I met with Dr Martin in his office in Oxford on Friday. We discussed planning for confirmation of status, a couple of conferences I want to submit papers to, and my seminar talk later today. I showed the call for papers for the VALID 2010 conference in August. The list of tracks is quite long and although it doesn't specifically include my area, I want to submit a paper nevertheless. I am thinking of an extended version of the ACSAC poster that was not accepted last December. The page limit is 6 pages, full paper, due 20th March. Dr Martin suggested I write an abstract and send it to the conference organisers earlier, to see if they say it's in scope for their conference. I will do that as soon as I get back to Colorado. I will also finish writing my Methodology chapter.

I reported the results of meeting with Julie Sheppard in the department regarding Confirmation of Status and extending my student visa in the UK. She wants the GSO.14 and MAT.3 forms filled out and signed no later than noughth week of Trinity term. Written work can be delivered to the assessors later. Confirmation must be achieved by the end of Trinity term which means before noughth week of Michaelmas term. In summary, paperwork in April for a viva in September. I characterised my seminar today as a good test for potential success in the confirmation process. If I can get a couple of papers accepted through the peer-review process by late summer, then that together with a finished methodology chapter and preliminary results will be my argument for the assessors in the confirmation viva. Today's seminar talk covers pretty much the same ground and is good practice for the viva.

Another conference I want to deliver a paper at is the UCDMO (Unified Cross Domain Management Office) conference in July. I have already been invited to prepare a paper; my question to Dr Martin was whether this conference would count, since it is a classified conference with a limited attendance and no proceedings published. Dr Martin asked me about the list of participants, and the programme committee of VALID 2010---was there any overlap? I did not recognise any names on the VALID 2010 committee, though I do know all the people in the UCDMO conference. Dr Martin said there was no problem publishing in a classified conference as long as my paper is approved for release.

I will email suggestions for new readings on the SPR course list soon.

Meeting ended 1129.

At 2:00 pm today I gave the first software engineering seminar of the term. There were about 13 people attending, some of whom had been there for last year's talk where I described earlier work on the same topic. I was pleased that Dr Simpson was there, as he examined me in my transfer viva. I started by thanking Dr Martin for being my supervisor and all the regulars at the Security Reading Group who get up early every week to talk to me on video. The title of my talk was 'Security Certification---You're Doing it Wrong'. The inverted commas refer not to the audience members who were listening to me talk today, but to certifying and accrediting agencies in the US Department of Defence.

I started out the talk with a little background, then I put my thesis statement on the big screen and invited people to throw rocks at it. I described my three thesis statements:

Firstly, the interesting situation:

1. What happens when an existing software system encounters security testing and evaluation criteria that are new or have suddenly changed?

Secondly, what I believe to be the root cause:

2. Certifiers and accreditors are conflating the practice of Independent Verification and Validation (IV&V) with the principle of defence in depth.

And finally, a quantitative question:

3. Is there a difference in the post CT&E software defect rate measured in terms of the number of findings of Category I, II, III, and IV between different versions of the same system in subsequent rounds of CT&E by different DAAs?

Earlier in the talk, I had described the unique CT&E problems of Cross-Domain systems (CDS), a particular species of classified information processing that I have some experience with. CDS encounter new or changed CT&E criteria about every week. As the final part of my dissertation I want to develop a software tool that will help lower the cost of CT&E of CDS by reducing the amount of duplicated effort. For example (an example that unfortunately I forgot to say during my talk), 110 of this type CDS were installed in 2009, at an average cost of $150,000. Forty to sixty percent of that cost went to IV&V, or $7,500,000, and this for a product with a total software development budget of only $2.1 million per year. It is a significant cost.

I stumbled once, but recovered from my notes and later in the talk I was speaking smoothly and without notes. Afterwards, Dr Martin said 'well done'. I talked for 50 minutes on the button, followed by questions. Questions included the correlation of CT&E findings in subsequent rounds, the order in which tests are performed, and Dr Martin brought up commercial auditors of data centres having multiple customers, the fact that it is well known that auditors always find something, and the leaving of 'crumbs' for auditors to find. I will research the existence of commercial standards for data centre auditing.

Next week Dr Martin will be in Florida, so our next meeting will be during the week of 1st March.

I have a meeting with Dr Ashbourn in ten minutes for college requirement.

Current list of tasks in order of priority, highest priority first:

1. Write abstract and send to VALID 2010 editor. 2. Methodology chapter 3. Renew student visa, including biometrics now required 4. CT&E practitioner survey (waiting until after 19th) 5. New (short) paper (interim???between these two) 6. Crosstalk article (concurrent with above) 7. Update schedule for Dr Martin 8. Apply for confirmation of status this term 9. Must have achieved confirmation of status by end of Trinity term

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

follow-up to weekly activity report 124 (loughry)
Joe Loughry
Sent: 19 February 2010 18:50
To: Niki.Trigoni@comlab.ox.ac.uk; Andrew Martin; Joanna Ashbourn
Cc: andrea@hpwtdogmom.org; Joe Loughry; mmcauliffesl@comcast.net
Attachments:

Dear readers of my weekly reports,

Late this afternoon I met with Dr Ashbourn for our annual review as required by the college. We discussed Confirmation of Status and she informed me it is possible to defer retroactively last Michaelmas term even at such a late date. She advised to do so in terms of risk reduction. I might not need that time now, but if things turned out later that I did need it, I would have it available.

The deferral would be for only one term, not a whole year, and would effectively give me until January (instead of September) to achieve Confirmation of Status. I would not change my plans or slow down, just remove the immediate danger of this deadline so I can concentrate on writing and have more progress to show at Confirmation time. It should not change my completion date at all.

I have decided to follow this advice and I will get that paperwork filed with the department immediately on Monday.

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

End of WAR 0124.

References