File 20100129.0358: Weekly activity report 0121:

weekly activity report 121 (loughry)
Joe Loughry
Sent: 29 January 2010 03:58
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. 20100128.1731 (GMT-7) sequence no. 0121, week 2 HT

I met with Dr Martin this week by video teleconference. We went through the latest outline of the methodology chapter and discussed a number of topics having to do with significance of results.

The 19th February seminar in Oxford is confirmed; I need to provide a title and abstract to the organiser in the next few days. I continue to expand the outline of my methodology chapter; a few paragraphs of the introduction are written but otherwise it is still in outline form. This morning I first wanted to talk about my null hypothesis. After I boiled it down to a single phrase in the introduction of the methodology, I worried that it began to sound trivial. Dr Martin helped me run it back a little from the too-short statement that I had, advising me not to pare it down quite so starkly as to lose all generality. The goal is to show evidence for a thesis general enough that it can be applied by other people to other problems in future with predictive value. I am going to work more on that straw man, as it is important to a convincing presentation.

Next we discussed various metrics available to measure both level-of-effort and security. We both agreed that the problem of how to measure and compare levels of information security is a hard one. It is not yet a solved problem and would be an important contribution itself to find one. I listed the available metrics for level-of-effort and asked Dr Martin for his opinion on whether any of them (calendar time, person-hours, total number of individuals involved, budget spent, number of test procedures, code coverage analysis) would be sufficient alone, or whether journal readers like seeing a synthetic measure better. Dr Martin pointed out that they are probably correlated anyway and I can easily look at them with a spreadsheet, compare and graph them and write an equation combining several to yield a strong synthetic measure if I need to later.

For measuring security improvement, I rather like number-of-findings-during-subsequent-testing. The nature of these software systems, ie cross domain solutions, is such that by definition they are installed across multiple security domains, each controlled by accreditors who do not necessarily trust one another. Hence the software tends to be tested and retested again using similar criteria but by different groups, eg FAT, IV&V, CT&E, and ST&E at multiple sites in the same security domain, followed shortly thereafter by new rounds of CT&E and ST&E in other security domains and by other certifiers. Nevertheless, testing criteria are often the same or similar, since NSA, NIST and GCHQ are the ultimate authorities on the subject of computer security. Different military standards tend to trace back to the same set of recommendations. This, I think is the best measure of security improvement that I can hope for---not one that is much applicable outside the peculiar environment I happen to be working in, but one that is highly applicable to certain situations---and most importantly, is available.

On the subject of availability, Dr Martin cautioned that getting statistics on the number of findings may be troublesome, but I do have access, and I think I can think I can get aggregate counts of Category I, Cat II, Cat III, and Cat IV findings released, if not identifying the system or version or patch level or application or site, and declassified so I can use them. It will require some negotiation with the data owners.

Another issue brought up by Dr Martin is the problem of measurement perturbing the thing being measured. I argued back that I think it won't be a problem because of the deliberate and careful separation that exists between each stage of testing: eg FAT, IV&V, CT&E, and ST&E. I think I can make a convincing case that Heisenberg uncertainty is not a problem here.

I would like to justify every step in my methodology as being both necessary and sufficient. The goal of this dissertation is to make a contribution that has predictive value, that others can use in future. I have added a new (small) section to the methodology, a preliminary survey of CT&E practitioners to establish what is known before my research gets published. As I said, I want to justify the existence of everything in the methodology as both necessary and sufficient; firstly, a survey to show that a problem is believed to exist. Secondly, a pair of case studies to show that the problem is real, but its behaviour is not consistent, so merely doing the opposite thing is not going to solve it. Finally, a prototype solution and validation that the prototype does (hopefully) work. If I can do all that it would be a contribution.

I asked whether this level of introspection, of discussing all the different alternatives, belongs in a methodology chapter. Dr Martin replied that if one of the main contributions of the dissertation is the methodology, then showing how it was developed and why certain alternatives were accepted or rejected does belong there. I was intrigued by this comment, and I think I may run with it some. I will explore it further in the next few days.

Plan for next few weeks: first, finish the methodology chapter and get it put to bed. Then prepare my talk for the 19th of next month. Immediately following, do that first survey. It is slightly unfortunate that I didn't identify the need until now, but it needs to be done, it needs to be done first, and it's simple and quick to do. I plan to have that completed in the next month. I need to consult with Dr Jirotka about the design of the questions. The next task is to update my schedule for Dr Martin. The first case study (Common Criteria) is largely written already; the second case study is in progress---successful so far, but still ongoing. I have not done much planning or detail on the prototype development phase at all.

We ran out of time this morning so I did not bring up the new paper that I was thinking last night of publishing. Dr Martin has been on my case a bit lately about publishing early and claiming the territory. I may have something I can publish soon. I may try to talk about that on Monday, or I may wait until I have it ready to show off.

Status: pressurised, but it is a good sort of pressure

Tasks in order of priority, highest priority first:

1. methodology chapter
2. Software Engineering talk (19th Feb)
3. CT&E practitioner survey (consult with Dr Jirotka on design of questionnaire)
4. First paper
5. Crosstalk article (to be submitted by 1st March)
6. Update schedule.

7. Apply for confirmation of status this term.
8. Must have achieved confirmation of status before end of Trinity term.

Next meeting: Monday, 1st February 2010 at 1715 GMT.

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

End of WAR 0121.

References