File 20100813.0519: Weekly activity report 0149:

weekly activity report 149 (loughry)
Joe Loughry
Sent: 13 August 2010 05:19
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

Weekly activity report no. 20100812.1959 (GMT-7) sequence no. 0149, week 8+8 TT

My submission to the SafeConfig 2010 workshop in Chicago was rejected.
The reviews were not too bad. One reviewer said that the problem was
interesting, just not central to the topic of the workshop (I figure
they probably settled on that only after seeing the mix of submissions
received). The second reviewer told me to send the paper to WEIS, as
that conference would be interested in it. I concur; the only reason
I did not send it there in the first place is because the conference
was already over. The third reviewer did not like my paper but from his
remarks I think he misunderstood it. I have a lot of additional material
I wanted to include in the paper; the page limit of this workshop was
too short and I had to leave out detail of my proposed solution because
of the necessity of setting up the background before I could explain it.
As I have lamented before, it is a problem with this whole sub-field; so
little has been published, I have to define terms before I can use them.
I have an entire mechanism yet to describe and I plan to do that in
a revised and extended version of this paper. It will be submitted to
ACSAC before the middle of September. In a longer format, I am confident
I can get this paper accepted.

This week I have been reading background material and doing miscellaneous
tasks. The UK border agency came back wanting more information on my
research topic before they will issue a new student visa. I talked
to Julie Sheppard and she provided a number of examples of acceptable
description paragraphs for this new requirement (called ATAS), which
applies to grad students in areas of transferable technology. I will
get that written tomorrow, and once Dr Martin has has a chance to look
it over, Julie will transmit it to ATAS. I spent a lot of time this
week preparing upcoming talks.

I think I am going to postpone my next trip to Oxford only a week or two.
The new date will be the second or third week of Michaelmas term---the
idea is to make it easier for other people to schedule around me. I need
to confirm status before the last week of Michaelmas term. That requires
written work, and forms to be submitted, and assessors to agree to do it.
As soon as I get back from France, I plan to begin submitting forms and
written work. As soon as Dr Martin returns from travel, I will discuss
it with him.

I learnt this week from reading Harland and Lorenz (2005) that systems
designed with failure tolerance to be able to work in degraded mode whilst
in a non-deployed or partially deployed state have saved many a mission.
I can think of analogies to the way software products are sometimes built:
sane defaults, live-CD distributions, and provision of a command-line
interface as backup to a GUI are all mechanisms I have seen included
in production systems but out of view of the end user, in anticipation
of problems. It would be far more difficult to design them in today,
as back then these features were specified by the set of requirements
that the programmers used, which were different from and more complete
than the requirements given by the business analysts. Such would never

be allowed in the environment I work in now. Implementation is always traced back to requirements, and functionality that cannot be traced is removed (McKinney, 2004). But in the early 1990s, we designed those features in illicitly as defence against disaster in the field. We did not have requirements auditors enforcing traceability then, but we also never encountered a disaster that we couldn't recover from.

Security Reading Group did not meet again this week, but I have been reviewing papers given to me by Shamal and Cornelius. A pile of books arrived from Amazon to be read; I have not gotten to them yet because I have been preparing to give two talks. Tomorrow, I am to give a talk to Lockheed engineers and customers on Gentry's fully homomorphic encryption, and in a week I have to leave for Nice. This will be the first time I have ever presented a paper at an international conference. I am working on making my presentation interesting. I have been told that the purpose of a conference presentation is not to read the paper to the audience, but to make them want to look up the paper and read it themselves. To this end, I plan to talk about the problem and my proposed solution in the larger context of my planned long-term research programme and why it is interesting beyond the present paper. Is it okay to talk about results outside the scope of a conference paper, if they relate to it because they are the next logical step beyond? I will dry-run the presentation with Dr Martin beforehand and ask him my questions. I have heard enough conference talks to know that the most interesting speakers touch only lightly on their paper---the audience perfectly well can read the paper if they want details. What they get in a conference talk is the high level view: why is it interesting, what were some of the problems encountered, what alternative approaches were tried and rejected, and why?

RM 5.0 ST&E is proceeding at STRATCOM. There was no telecon this week amongst the developer, certifier, and programme office because many of the participants are attending the UCDMO meeting in Boston. Those at the conference were planning to discuss it informally, probably at dinner tonight. I have asked several people in the group to bring me back impressions of that meeting if it occurs. The next planned telecon is a classified discussion on 19th August to look at the results from ST&E and solicit concurrence on accreditation and baseline decisions. At the present time, reports indicate that ST&E is going smoothly.

No replies from US government accreditors this week regarding contacts; many of them are attending the UCDMO conference; other are knowns to be tied up in ST&E this week. I will ping them again after next week, beginning Monday the 16th.

My current task list (in priority order, most urgent first):

1. Finish preparing presentation and talk for Nice. Give talk at Lockheed tomorrow.
2. Continue arranging appointments with Paul Ozura, Frank Sinkular, Dan Nichols, and Dave Wallick in D.C. in early October.
3. Install Matlab and code the numerical model for risk--effort pricing equation. Code acid tests. Find an equilibrium and fill in the blanks in the draft paper.
4. Fill out forms for confirmation of status. Schedule a meeting with Dr Martin to look at written work.
5. I am working on the Crosstalk article again. I have an idea how to explain the first case study in terms of accreditor behaviour incentives.
6. Send out second group of US government accreditor surveys. Look for UK government accreditor names in project records.
7. Get the other two surveys done for background on the case studies.

```
8. Make a fault-tree diagram for R-prime and S-star.
9. Draw up an org chart for R-prime, S-star, and G.
10. Finish methodology chapter (waiting on final survey questions).
11. Write first draft of confirmation report and send to Dr Martin.

To be done as soon as possible:

12. Update dissertation Table of Contents.
13. For Chapter 3 or 4, start writing the interpretation of the first
case study results and second case study preliminary results.
14. Compare NIST SP 800-53A to ISO 27001/2.
15. Update the schedule.
16. Submit forms and written work for confirmation of status during
Michaelmas term.

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

End of WAR 0149.

References