File 20100611.0348: Weekly activity report 0140:

```
weekly activity report 140 (loughry)
Joe Loughry
You forwarded this message on 11/06/2010 23:23.
Sent: 11 June 2010 03:48
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. 20100610.1822 (GMT-7) sequence no. 0140, week 7 TT

I registered my revised abstract with the 2nd ACM Workshop on
Assurable and Usable Security (SafeConfig).  This is the paper that was
rejected from the UCDMO conference, but it contains new material on
my proposed solution for improving a non-optimal equilibrium amongst
$n$ accreditors of a CDS installation connected at widely different
security classifications.  The deadline for full papers is 28th June.
I will work on it Sunday.

Regression testing of Change Requests (CRs) in response to Beta 1 CT&E
findings has been under way all week.  All of the IV&V contractors are
in Denver; they worked all weekend and some of them (the Test Director,
Kori Phillips) worked all night.  Regression testing was not going
well as of Monday night.  Two major new features are being tested,
and one is not working.  One of the features was added in response to a
'high' importance finding during Beta 1 CT&E; that feature is working.
The other major new feature was added by the developer two months ago (at
the direction of the PMO); it is this latter feature that is not working.
The developer lacks the option of dropping the second new feature
because it replaces old functionality that was removed two months ago.
I apologise for being vague here but the identity of the new features
is not important and they may contain security-relevant and proprietary
information.  Both of the problems are interesting because they show
the effect of late software changes at an extremely time-critical point
during CT&E.  Less important changes would be backed out and not allowed
to possibly affect the certification schedule.

Next week the developer will ship equipment to SSC Charleston and
Washington, DC.  This will be followed by three weeks of government
regression testing.  To save time, the developer is having IV&V witness
some of the regression testing in Denver this week---with the agreement
of the certifier that it will allow that portion of the government
regression testing to be skipped in Charleston, as it will have already
been performed and witnessed by IV&V.  Three weeks of government
regression testing will be followed by ST&E at STRATCOM (Beta 2).
STRATCOM is bending over backwards to help.  ST&E will be followed by
penetration testing at a live site, not yet named.  The developer expects
to receive approval-to-field on 20th August; the schedule has not slipped.
Incidentally, I want to take a look at current and old versions of the
schedule to see whether any slack time was designed into the schedule at
the beginning.  I suspect not, based on two pieces of evidence: firstly,
the fact that CT&E has stuck precisely to the schedule with no slips,
despite extremely tight funding at times; and secondly, some comments
from the penetration testers last month.  In the schedule, 5.0ZC is the
last build before the developer fields it.

There were two classified telecons this week, on Monday and Thursday.
In attendance on the call Monday were I173, Corinne, PMO, Don Nichols, Don
Capanero (sp?), Dennis Bowden, Orville, Paul Ozura, Ian, Kevin, myself,
```

Olav, Emily, Dan Griffin, Lisa Ackerman, and Larry Sampson. Charissa, Galena, and Atri were not available. The call was short in duration, covering refresh of both labs and Charleston. The equipment will be shipped from Denver next week. Installation is planned for week of 21st June. Internal regression testing of the 22 CRs is happening this week in Denver by PMO and IV&V. Accenture is the IV&V contractor. There was discussion of security coordination (visitor requests) for installation at STRATCOM. No changes were made to the schedule. One participant on the phone asked if there is a NIST standard for the format of a POA&M, but no one knew the answer. Another person on the phone asked about posting of the RM 5.0 test procedures for the CDS community. That was deferred for later consideration after they are not so busy.

I had a face-to-face meeting with Mr Ozura after the second telecon on Thursday morning. He is in Denver with the IV&V team. He wanted to talk about my questions regarding multiple DAAs. Sometimes, he explained, an MOA (Memorandum of Agreement) will specify which DAA is in charge. Other times, especially if at least one interface of a CDS is connected to SCI, the DAA on that side will announce that he or she is taking responsibility. Other times, a CDMO or the UCDMO may decide. On rare occasions, the decision goes all the way up to the PAAs (DNI). Mr Ozura is going to give me a more detailed written answer to my emailed questions in a few days.

I described to him what I am doing and explained why I am observing the RM 5.0 CT&E process. We discussed the politics that we had both witnessed on the telecon, some of the personalities involved, and various reasons why they might be doing some of the things they are doing. I explained that I have limited time to study the evolution of projects that might take years to unfold, so I am building a model of the (DAA^n)--developer world that is abstract enough to show all the possible interactions but simple enough that I can prove things about it. Mr Ozura suggested that I should continue this line of research as a postdoc. He is very interested in seeing an improved method to be adopted. He suggested I keep working on it for the next five years.

He recommended that I speak with Dave Wallick, the chief of the Navy CDSO. Mr Ozura described him as the most level-headed, intelligent person in the business; Atri works for Dave. I should tell Mr Wallick that Mr Ozura pointed me in his direction. It may be difficult to get together with him, but following CDTAB (a monthly event) would be a good time. I should try to get him away from the office in an unclassified setting and ask my questions there. Mr Wallick is also a CISSP-ISSEP.

I am willing to fly out to the east coast to talk to Mr Wallick, especially if I could arrange to meet with several other people in the same trip. I will ask the PMO to arrange for me to be able to attend an upcoming CDTAB.

Before I meet with Mr Wallick, I was advised first to talk with Frank Sinkular and Dan Nichols. Mr Ozura says that these gentlemen are thoughtful practitioners and would enjoy talking with a PhD student. I should ask them about 800-53, find out their questions, observations, and concerns. I should also ask them who else they would recommend I talk to.

Mr Ozura provided the validation I needed that my model of multiple DAA interactions in cross domain CT&E is correct. He said it fairly reflects the way real accreditations have been structured in his experience. He wanted to talk about DAA--DAA interactions where accreditor A has information but will not share it with accreditor B because of

a turf war. This is slightly different from my theoretical scenario, but does closely mirror observed interactions during the 5.0 CT&E, and I think I can figure the concept of turf war in a similar way to security clearance. Personally, I despair of achieving a complete understanding of the politics going on in that room. I can describe what happens, I can make hypotheses about patterns that I have observed across two case studies, and I can test hypotheses on my abstract model. If I can finally make predictions about the behaviour of future ST&E efforts based on it, then I will have achieved something.

The second telecon this week took place on Thursday. The meeting is referred to as a 'hotwash' although I am not sure of the etymology of that term. Present or on the phone were myself, Rob Drake, Corinne, Kevin Miller, Dennis Bowden, Orville, Ian, Olav, I173, DNI CAT, Larry Brown, and Paul Ozura. The meeting began with discussion of a revised format for the POA&M. Emily reported that pen testing findings were in the spreadsheet. Corinne wants to provide comments on some of the suggested mitigations. The developer is recommending that in some cases a feature not be used, and to document that, and call it a mitigation. Corinne says that some of these mitigations are unacceptable, and wants to give guidance to the PMO on mitigation. Charissa and Atri will assign priority numbers to all of the items by tomorrow.

The time for discussing mitigations is getting short: Kori Phillips will be in SSC Charleston, and Kevin Miller at NSA (Emily's place) the week of 21st June. Mr Bowden made a general comment on the six hundred or so 800-53 security controls: 'We think it is maybe a burden on the sites to answer a couple of hundred questions. It is a burden on the operational sites. The data are there, it is just that gathering it is a burden. Because part of this CT&E effort is to assess how 800-53 works in the CDS accreditation process, and because the CDMO is the face to the sites, they come back to the CDMO with their complaints, not to the CTSG or the UCDMO.'

Paul Ozura said that he is currently making a spreadsheet of 800-53 security controls and converting it into an automated tick-list for the sites. It will be ready at the end of this month.

The week of the 21st, Mr Bowden is hopeful of sitting down with the pen testers and showing them things in their own lab. This is hoped to defuse some of the risk mitigation disagreements.

Other activity this week: I found a video of a 2006 talk given by Sir Tony Hoare. His advice for PhD students in computer science: emphasise the limitations of your own work. Talk up the merits of previous work; your own small contribution can then be seen as an improvement to something that was already good. It will keep those earlier workers on your side. Never claim to be useful when you are working in science.

I am scheduled to give two talks at Lockheed in a few days, one on technology for privacy protection and the other on current topics in emanations security.

Administration: I submitted my GSS report on time. I had no meeting with Dr Martin this week because he is teaching, but I was at the Deer Creek Facility a lot of the time anyway. The schedule of talks for the conference in France came out this week, and mine appears in it. I conclude that editors were satisfied with the final version of my paper. I have a question, though: do I need a visa to go to France for a conference? I am trying to find out from the French consulate whether presenting at a conference counts as teaching. If anyone with more

experience presenting at international academic conferences has advice, I could use it. What do you tell the border guard? Is it considered a business trip?

Reading Group this week discussed Cormac Herley's paper from NSPW'09 on rational rejection of security advice. The paper contains some ideas I can use: constrained optimisation in Section 7.4, and prioritising of security advice in Section 7.6. Users, he says, are not offered security, but rather 'long, complex and growing sets of mandates, policy updates and tips. These sometimes carry vague and tentative suggestions of reduced risk, never security.' [Herley, 2009] In the references is an interesting paper by Beautement, Sasse, and Wonham ('The Compliance Budget', NSPW 2008) that I am currently reading.

Dr Martin is teaching this week but I will schedule a meeting next 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 paperwork is still due. 3. Outline the ACM paper on improving a non-optimal equilibrium amongst accreditors. 4. Talk to Paul Ozura more about it. 5. Transfer list of accreditor meeting attendees and email addresses into a searchable text file. 6. Ask PMO for an invitation to attend next CDTAB, or the one after that. 7. Finalise 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 the first case study results and second case study preliminary results. (This will be needed for both confirmation of status and for answering questions in France.) 12. Document the codes used 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 0140.

References