File 20100730.0423: Weekly activity report 0147:

weekly activity report 147 (loughry)
Joe Loughry
Sent: 30 July 2010 04:23
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
Attachments:
Weekly activity report no. 20100729.1454 (GMT-7) sequence no. 0147, week 8+6 TT

I feel that I know precisely what I need to accomplish between now and confirmation of status. I have a fairly good idea of what the finished thesis will look like. I have started writing a confirmation report in parallel with working out the problems of the accreditor model. I have been thinking about accreditor interactions in my head, not in Matlab yet. I need to get it reduced to equations soon. I have been reading articles on game theory, looking for something like a closed-form solution I can use. So far, I think it is analogous to---although definitely not the same as---a Cournot game. At least there are strong parallels in the analogy to accreditors' desire to minimise residual risk and the ways in which they may offer to cooperate. I am going on the assumption, after a disagreement with Shamal over the idea, that cooperation in the accreditor model is dual to competition in the Cournot game, and that an equal and opposite force can drive an equilibrium just as strongly. I really need to study more microeconomics.

I found a reference in a recent article by Thompson to a 1982 report by Jacques S. Gansler about the defence industry. I have a copy on order from a used book dealer. The report deals with the unusual relationship between government and defence contractors and characteristics that lead to high cost of things like cross domain systems. A modern example is the F-22 Raptor: there is only one customer, the US Air Force, because the US government prohibits sale of the fighter to other countries. Some CDSs are in a similar position. If I intend to make the claim that the cost of CT&E and ST&E of CDSs is too high at present, and that I have a solution that preserves the security property, I must somehow make it square with Gansler's earlier analysis of a something related. There is an extensive literature on weapons system procurement (unlike anything to do with CDS) that I can draw from. Fortunately, I have already read a lot of those books (Stevenson, 2001; Whittle, 2010; Burton1993; Westrum, 1999; Lundstrom, 1987; Brown, 1999; Redmond, 2000; Dyson, 2003; Boslaugh, 1999; Reed, 2004; Clark, 1972; Dequasie, 1991; McKinney, 2004). I have been reading Harland and Lorenz (2005) on the faster-better-cheaper experiment that NASA tried, beginning in the early 1990s. The necessity for high fidelity testing and design for reliability are both familiar concepts that are as applicable to CDSs as they are to spacecraft. (I wonder if there are anything like accreditors for spacecraft? Must check.)

There was no Security Reading Group meeting this week, as Cornelius has a new paper that he is sending around for comments. I did not meet with Dr Martin this week because he is on holiday. I spent a day and a half reorganising my files, pulling together a bunch of old notes that I had written in different places into a single, searchable file, sorted chronologically. Now that the second case study data are sorted, I need to do the same thing with the first case study data. I also need to get more accreditor surveys out to people.

I need to write my presentation and talk for the conference in Nice.

Some of it is familiar material I have presented before, but I want to talk about the accreditor model and the design of the tool also. Part of the reason for this is a dry-run for confirmation in October. I am planning a trip to Oxford around the middle of October, on my way back from talking to accreditors in Washington, D.C. I hope to schedule a confirmation of status viva at that time. For reasons of security classification, export control, ITAR, and proprietary information, I am leaning more and more in the direction of developing the theoretical model of accreditor behaviour (backed up by interpretation of the two case studies) specifically because it is abstract. Let me explain. If it is abstract it goes under the radar of managers at work. I can work on it without being pressured to develop it into a proprietary product. By developing a useful tool whilst disguised as a mathematical problem, I can finish this in time without their interference. But I am still talking with accreditors on a daily basis about their job.

The RM 5.0 certification test and evaluation process is moving towards a successful conclusion. The developer has received drafts of the final NSA penetration testing report and government regression testing report from Beta 1 CT&E. There are no surprises. The developer has fixed all of the issues that they chose to fix, and documented the others. There was a 5.01 patch preliminary build meeting this week to approve files that will go into the POA&M patch; no date has been decided yet for when the patch will be issued, except that it will be after 20th August. The developer continues to express the feeling that one person at NSA has a bias against RM and will always find something wrong with it. It is my perception, however, that that person is only one vote amongst the group that decides the outcome of the CT&E, and either lacks the power to stop it, or has been sufficiently appeased, or is being ignored. Deeper analysis of that awaits more data.

Present on the call today were Dennis Bowden, RM programme office; Larry Sampson, Unified Cross Domain Management Office (UCDMO); Larry Brown, Kevin Miller and Ian McGlothlin, Lockheed Martin; Dan Nichols,Unified Cross Domain Management Office (UCDMO); Charissa Robinson, NSA I173; Kevin Gallicchio, NSA I733; Dave Oshman, NSA I173; Dan Griffin, US Navy SPAWARSYSCEN-Pacific; Maureen Branch; Corinne Castanza, DNI CAT; and myself.

Charissa from NSA I173 will send out the final CT&E regression test report from SSC Charleston by close of business tomorrow. Dan Griffin just got back from STRATCOM and reports that all is going well; they will be ready for UCDMO to arrive and for ST&E to begin next week. Larry Sampson then asked if there were any additional comments on the report.

Kevin Gallicchio reported that the latest patch received from the vendor was tested. It successfully corrected both [redacted] and [redacted] issues.

Dennis Bowden asked a question about the body of evidence he is assembling: is there an equivalent to the unclassified SharePoint server where all of these documents can be posted so that people who only have access to JWICS or SIPRNET can read them without having to email files around all the time? Mr Sampson replied that there is a classified server and space would be set aside soon.

Regarding the schedule, on Monday next the Beta 2 phase officially begins with ST&E at STRATCOM. Geoff McGarrigle from the RM programme office will be there; Rob Drake from DIA will be there; Russ Savage and Kori Phillips from the developer will be there. Don Flint and Corinne Castanza from DNI CAT will arrive the week of 16th August.

The first few SABI installations after ST&E at STRATCOM will have the hardest time getting through the CDTAB and DSAWG process, observed Dennis Bowden. We shall have to look hard at the body of evidence for those first sites. Charissa Robinson asked about the patches called for in the POA&M: SABI sites will have a very different configuration from STRATCOM [Editorial note: STRATCOM is essentially a TSABI site] but will not every change listed in the POA&M have to be tested? Dennis Bowden replied that the POA&M will come with a single common patch CD for all sites; all sites will have to be updated per the POA&M, so all will have to be tested for all POA&M-changed functionality.

Kevin Miller is going to wait for Kevin Gallicchio's final report before making the final developer updates to the POA&M. That report will come out next week.

Charissa Robinson will be doing a Test Readiness Review (TRR) for CDTAB in September. In preparation for that, she is looking at the entire body of evidence that they have created, RDAC and RMF.

Dennis Bowden: It is the position of the Radiant Mercury Programme Office that the first few SABI sites can proceed with the first certified RM 5.0 software version in advance of the POA\&M patch, although possibly with a higher risk assessment. Charissa Robinson replied that it is an accreditation decision; it cannot be made without a risk assessment. Corinne Castanza noted that she is finishing up for DNI CAT a complete list of findings, annotated with the latest developer responses and NSA replies to the response, consistent with both risk assessments, for the body of evidence used to create the report. Charissa Robinson concurred and stated that NSA I173 will do the same.

Will it be possible for Dennis Bowden or another Programme Office representative to attend the CDTAB? Charissa Robinson will try to get an invitation to the CDTAB, although the CDTAB does not usually entertain visitors. Dennis Bowden observed that IV&V is more likely to be invited, since they are totally independent of Lockheed Martin, but IV\&V may not be available this CDTAB because of scheduling conflicts. Charissa Robinson said that because this is the first time for a new CT&E standard, it is possible that others might be able to get an invitation to CDTAB. She will check on it.

Paul Ozura has on his to-do list to check over all the old items on the findings list, to verify that no findings have been forgotten and that all software changes have been tested, for example the [redacted]. Kevin Miller described the fix for that issue, which is a procedural change only and entails no code changes.

Dan Nichols requested a sidebar with Dan Griffin and Dennis Bowden at the CDMO Conference, the week after next.

Call ended 1025 EDT with the observation that because STRATCOM will be testing next week, there likely will not be a classified hotwash telecon next week, but there may be an unclassified one. Larry Sampson will send out an announcement early next week.

After the telecon, Larry Brown noted that this was the best meeting yet. It looks like it is actually going to happen. [Editorial note: the upcoming ST&E at STRATCOM is something the developer has the ultimate amount of experience with. I can foresee no way it could be anything other than successful. The mechanism is solid, the problem is well understood and all the testers and certifiers have been involved in it for a year. The people doing the installation and testing are highly experienced.]

Kevin Miller brought up the fact that the Legal department of Lockheed Martin should be consulted regarding source code changes to the COTS software that Eric developed in the process of fixing the SNMP problem (three JAR files). Those code changes should be released back to the community. The developer is going to do it.

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

1. Continue arranging appointments with Paul Ozura, Frank Sinkular, Dan Nichols, and Dave Wallick in D.C. in early October.
2. Implement a numerical model for the risk--effort pricing equation in Matlab. Verify that acid tests hold. Extend the paper with the new results.
3. Prepare presentation and talk for Nice in three weeks.
4. 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.
5. Accreditor surveys. I understand the problem much better now. I need to be able to describe these surveys in the Crosstalk paper.
6. Get the other two surveys done for background on the case studies.
7. Finish methodology chapter (waiting on final survey questions).
8. Write first draft of confirmation report and send to Dr Martin.
9. Prepare talk for 13th August at Lockheed on crypto maths.

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 likely audience questions in France.)
12. Compare NIST SP 800-53A to ISO 27001/2.
13. Update the schedule.
14. Apply for confirmation of status; submit written work.

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

End of WAR 0147.

References