File 20100416.0619: Weekly activity report 0132:

```
weekly activity report 132 (loughry)
Joe Loughry
Sent: 16 April 2010 06:19
To: Niki.Trigoni@comlab.ox.ac.uk; Andrew Martin; Joanna Ashbourn
Cc: otaschner@aol.com; andrea@hpwtdogmom.org; chip.w.auten@lmco.com; diane@dldrncs.com;
Joe Loughry; mmcauliffesl@comcast.net
Attachments:
Weekly activity report no. 20100415.2156 (GMT-7) sequence no. 0132, week -1 TT

I have long been planning to submit a paper to the 4th Unified Cross
Domain Management Office (UCDMO) Conference, 9--12 August in Boston,
Massachusetts.  Yesterday I finally tracked down the call for papers,
which is not published in the usual channels.  I almost missed the
deadline.  Tomorrow is the deadline for abstracts, and I want to submit
the following:

Title: Information Asymmetry in Cross Domain Accreditation

Abstract: The theoretical difficulty of cross domain systems emerges
from the fact that by definition they span at least one boundary between
security domains controlled by different data owners.  Consequently, new
installations of certified solutions regularly encounter security testing
criteria that represent the duplicated responsibility for residual risk
of multiple data owners.  Each data owner perceives a different set of
risks $A$ that would be desirable to mitigate, a set of risks $B$ it is
possible to mitigate, and their relative complement $A - B$, being the set
of residual risks acceptable not to mitigate.  Time and cost inefficiency
in multi-lateral cross domain system accreditation to this point arises
necessarily from asymmetry of knowledge, but there is room for a solution:
the developer or installer of a cross domain system may know about extant
risk mitigations that not all data owners are cleared for.  If it were
possible securely to establish amongst data owners a concord about the
true extent of residual risk resulting from overlapping risk mitigations
and testing, the unnecessary cost of duplicated effort could be greatly
reduced.  In support of this goal, a new tool, called {\it nihil obstat},
is being developed to present accreditation data in a common format.

Only the abstract is due at this time.  The abstract has been submitted
for classification review.  The conference organisers request that
submissions be either PowerPoint presentations or lectures; I am writing
this paper as a lecture.  It is also a section of my dissertation.
I found another section today that can be published as a stand-alone
paper as well, on the overlap with safety-critical principles.

The intent of this paper will be to lay out the theory behind my
thesis, that overlapping areas of interest inherent to any cross-domain
accreditation necessarily lead (at least the way it's done today) to
duplication of effort and consequently inefficiency.  It is unavoidable
due to the structure.  I propose a solution that turns the problem
inside-out by taking advantage of the 'privileged' position of the
developer or installer, which until now has appeared to be either
passive or actually disadvantaged.  I believe that if the developer
or installer would only use the quasi-omniscient knowledge that they
must necessarily possess, but that various data owners either do not
know that the developer possesses or are not cleared to know, that the
full accreditation can be streamlined saving everyone time and money.
I did not see how to do it until just now.

I met with Dr Martin yesterday morning.  I reported the current status of
```

Radiant Mercury 5.0 certification testing; the IV&V team in Charleston, North Carolina is wrapping up and will be finished with their testing on Friday of this week or Tuesday of next week. They will then write their report, due 30th April. Penetration testing at Ft Meade is still ongoing. They won't stop until ordered to stop and write a report. Unlike the IV&V group who have a finite number of test procedures to go through, pen testing is completely open-ended and doesn't stop until they run out of money. It is very similar to covert channel analysis (CCA) in that way.

The IV&V report will come to the developer and the certifier at the same time. The developer will spend a couple of days reading and understanding the report, then probably have to develop a patch for any Cat I or Cat II findings from CT&E. Issuance of the patch will be followed by commencement of the final stage of testing: Beta 2 in an operational environment.

The plan calls for Beta 2 testing to be done at Joint Forces Command, but I am aware that JFCOM has a time constraint. Beta 2 must be complete by 1st June because they need to support an exercise at that time. Between 30th April and 1st June there is not enough time for the developer to receive the IV&V report, develop a patch, get it into testing at JFCOM, and finish by 1st June. So the developer and the programme office have formulated two alternative plans: either wait until August when JFCOM will become available again, or move the Beta 2 testing to STRATCOM instead.

Neither of these backup plans is very desirable, but I predict they will choose not to wait. Waiting until August for Beta 2 would delay certification, and that would impact the plans of multiple customers who are counting on getting certified RM 5.0 systems this summer. I predict that the programme office will do two things. First, they will try to cram Beta 2 into JFCOM before the deadline. They will waste some time trying to do so, and the certifier will tell them to back off. Then they will move Beta 2 testing to STRATCOM to avoid delaying the certification.

It is expected that no major findings will result from Beta 2. There is the possibility of a patch, which would necessitate re-running regression and IV&V tests, but that is unlikely. After Beta 2 finishes, and the operational site submits their report to the certifier, then it is only a short time before a certification letter will be issued. UCDMO will announce version 3.3 of the list of approved guards, and installations at operational sites will be able to proceed as scheduled.

Documentation of the above series of events is interesting for my thesis because it illustrates how the certification process actually works in practice.

Next, I reported on progress achieved during the past two weeks. I have been taking a lot of on-line surveys, examining how the questions are worded and arranged in an attempt to learn the tricks. The survey software provider has a tutorial available, which I went through, and there are several web-based courses from other providers. I want to get the survey questions out to my test participants in the next 6 days. Update: because of the UCDMO deadline, I spent a day and a half writing that abstract instead. I also have to prepare for my next talk at Lockheed in four days. I will get the surveys done as soon as possible.

Regarding the Venn diagram that appears in the VALID 2010 paper: anticipating something I expect to happen in future, I have been formulating an answer to the question I expect to be asked some day: 'tell me what it means'. I have been thinking about how to explain it with overlays or animation.

Other than the above, I spent a lot of time reading last week, mostly on safety-critical design, but also a criticism of safety-critical principles applied to security-critical systems (Johnston, 2009a). The talk I gave at Lockheed was well-received, resulting in an email in-box full of requests for more information and requests for more talks. I have three more talks scheduled, on 20th April, 23rd or 30th April, and 5th May 2010. It is good experience in both speaking and writing.

I reported some frustration with the Lockheed process of review for public release. In the past it was relatively quick, but lately the queue has bogged down and I have several requests in the pipeline that haven't come out yet. I am not sure whether the person who does it has changed jobs or what, but I need to visit the Deer Creek facility later to find out. It is not impacting the schedule yet but the lead time is a possible risk for upcoming deliverables.

Looking at the schedule, Dr Martin observed that the Crosstalk journal paper has been 'two weeks out' for a long time now. Looking at the schedule, we re-prioritised events as follows:

First, get the surveys out. They represent data, which I need for interpreting preliminary results in the journal article. Additionally, the survey design is part of the methodology, needed also for the Crosstalk article submission and methodology chapter.

Next, complete part of the methodology chapter followed by getting the journal article out the door. I need to look at the list of priority tasks in Gantt chart form, because there are interrelationships between tasks that do not show up in list form. Dr Martin cautioned not to spend much time over-thinking the schedule, though. Results are needed more.

The feeling of sending out a paper for publication is good. That positive reinforcement is what keeps me going forward. My proclivity is to delay by over-thinking, over-planning, or by finding another paper to read instead of writing. I have to control that tendency.

Dr Martin said I appear to be on a roll, slightly in danger of falling off but not fallen off yet. Get some concrete results from those surveys and I will be in better shape. Dr Martin said that getting a stack of survey results back will be good positive reinforcement.

Next meeting scheduled for Wednesday, 21st April at 1400 Oxford time.

Current list of tasks in priority order, most urgent priority first:

1. UCDMO conference abstract due tomorrow. 2. Email addresses for practitioner survey, participant survey, and user survey; develop questions, enter in SurveyMonkey and test. Goal is 20th April. 3. Prepare for Lockheed talk on 20th April. 4. Write methodology chapter. 5. Finish preparing Part 2 of C&A talk for Lockheed. 6. Journal article (based on methodology chapter, extended version of the VALID 2010 paper and recent talks) now to be submitted before 30th April. 7. UCDMO full paper for August conference; deadline not announced yet. 8. Update Table of Contents. 9. Begin writing progress report for confirmation of status. 10. Fill out paperwork for UK student visa extension in April for June application deadline. 11. Update the schedule. 12. Apply for confirmation of status---I want to submit the forms with written work in June for August or September. 13. Development of accreditor information coordination tool: design as described in UCDMO paper.

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

End of WAR 0132.

References