File 20100903.0346: Weekly activity report 0152:

```
weekly activity report 152 (loughry)
Joe Loughry
Sent:  03 September 2010 03:46
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. 20100902.1250 (GMT+1) sequence no. 0152, week 8+11 TT

I have been working on a vector representation for accreditor work units.
The basic operations of bid, ask, and post (a type of commit operation)
are sort of working now; I found early on, however, that an option
mechanism is going to be absolutely necessary or the whole thing reduces
to a FIFO queue---not very interesting.  Options make it multidimensional
in time: a little like quantum computing, or speculative execution in
a pipelined processor.  Security clearance and security classification
are zeroed out at the moment because I am not sure how to handle those
relations yet; I will have it figured out in a few days.  The submission
deadline for the ACSAC conference is 17th September; I would like to
get the revised paper containing this idea submitted there.  If not,
then I have a backup plan: the 12th IFIP/IEEE International Symposium on
Integrated Network Management.  One or the other of these conferences
ought to accept the manuscript.  The acceptance rate of ACSAC is less
than 20 percent; I have not been able to find data for the acceptance
rate of IM 2009.

In my talk last week, post last week's report, I had some discussions with
people who asked more questions about the first case study I presented.
I have nearly gone through the alphabet choosing anonymisation codes;
I thought there were too many but the people felt it was understandable
and wanted to see a few more.  The people picked up on the core idea
immediately---that accreditors from different agencies were not talking to
their counterparts.  I did not lead the audience to that interpretation;
I was talking about something else when they began to ask those questions,
which leads me to believe it's a good independent validation.  Besides
additional anonymisation codes (they wanted to see the influence diagram
extended to include predecessor and successor systems), I have categorised
five reasons why accreditors do not communicate: Country, Corporation
(this also includes agency, department, and military service branch),
Contract, Clearance, or Classification.  I have seen examples of all of
these in observations of R-prime and R-double-prime.

I was unable to attend the RM 5.0 CT&E telecon last week, but received
an unclassified report of the event from participants.  Rob Drake and
Corinne Castanza (DNI) reviewed the results of ST&E penetration testing
of the installation at STRATCOM.  The 1st October date for UCDMO baseline
listing, as of last week, was expected to slip, to the consternation
of the PMO.  DNI was unsure as to who would accredit the STRATCOM site,
and that opened a can of worms.  Last week's meeting was not a good one,
overall.  In contrast, today's telecon went well.  Present on the call
this morning were Kevin Miller, myself, Don Flint, Rob Drake, Dennis
Bowden, Larry Sampson (moderating), Jake Randall, Charissa Robinson, Dan
Nichols, Dave Oshman, Dan Griffin, Olav Kjono, and Lisa Ackerman, but no
one from the NSA pen test organisation.  Rob Drake began with a review
of his preliminary ST&E report and POA&M validation, highlighting three
categories of CT&E items as he saw them: (A) items that can be closed,
(B) items that he wants to give another look, and (C) items that remain
open but are covered by the POA&M mitigation plan.  In the validation
```

report, fifteen or so category A items have been closed entirely; those vulnerabilities no longer exist and this fact has been validated. Of the items in category C that remain open, all are addressed by the POA&M. Category B lists failed security controls that he wants to look at again; some of these are instances where the system is working as designed; others are vulnerabilities that cannot be fixed for technical reasons. Either way, they are not findings; according to Mr Drake, something that cannot be validated cannot be considered a finding.

Regarding the ST&E and (STRATCOM) pen test reports, UCDMO requested that the two reports not be combined. To make information more clear for the baseline, the pen test report will be divided into two parts: CDS-relevant findings and site-relevant findings.

Dennis Bowden asked about a certification or CT&E letter. Rob Drake said he intends to put out an accreditation letter soon. Each agency, e.g., DIA, will issue its own accreditation letter. They do not indicate a type accreditation, merely that RM 5.0 has been tested and certified in one instance. The letter is not site specific; the generic accreditation letter is intended to feed into every site's Body of Evidence (BOE). For its BOE, for example, DIA will be using the old SSAA, among other pieces. Once the DIA CIO leads with the letter, DSAWG looks at the BOE plus their own BOE, considers everything, and decides whether to put the CDS on the baseline. DSAWG requires one ATO as part of a BOE to go forward with placing RM 5.0 on the baseline. Currently there is an interim (three-month) ATO at STRATCOM because they do not yet have a full BOE. Specifically, the 800-53 report is not yet finalised; that is the only thing holding the accreditors back from issuing a full three-year ATO.

There followed a three-way discussion amongst Dennis Bowden, Dan Nichols, and Charissa Robinson about whether the BOE should include a long form SSAA or the new SSP. Answer: UCDMO will accept either SSAA or SSP; there is no need to duplicate effort by preparing both. Dennis Bowden will continue polishing the long form SSAA. Mr Bowden asked if a SharePoint site has been set up yet for collating BOE documents; Mr Nichols stated that UCDMO needs to receive the documents themselves, not a pointer to a web site. The reasoning is that UCDMO cannot publish the BOE, because they are not UCDMO's documents to distribute. UCDMO is unable to act as the repository for collecting documents; nevertheless, UCDMO insists that it must receive BOE documents directly from the government, i.e., Dan Griffin. Dennis Bowden may prepare it for Dan Griffin but the PMO must transmit the BOE to UCDMO.

Charissa Robinson asked about having a Lockheed Martin engineer at the CDTAB on 21st September. CDTAB members will likely be very curious and will ask many questions about internal processes comprising the guard, how those processes communicate, use of privilege in the OS, and so on. It would be highly beneficial to have there an engineer available who is familiar with the internals of the software, not just with the test procedures. This resulted in some discussion; it is unusual to have developer representation at CDTAB, but the present situation is unusual, giving that the certifiers are learning the a new process as they go along. The developer agreed to provide an engineer; IV&V will also send representation along.

[Editorial note: immediately after the telecon I requested to go along. The invitation to attend CDTAB is unprecedented---developer representatives are never allowed in to these deliberations. I put forth that it might be politically more acceptable for me to show up in the role of a Lockheed Martin IA engineer, rather than as an outside observer, but

either way I wanted in. Within a few hours I had an answer: probably no. The programme manager believes that CDTAB will be reluctant to admit even two LM engineers or one LM engineer and one IV&V representative. So it looks like it might not be possible to see inside. The request to attend will be made, but he is not sanguine about the chances. As of late tonight neither of us have given up, though. I just hope the decision doesn't come down to the wire like the UCDMOC did; last-minute travel to Washington, D.C. is extremely expensive.]

Rob Drake promised that the ST&E test report will be available next week. He is doing housekeeping details on it now. It will be delivered by 10th September. Larry Sampson will send out a matrix to all participants detailing all items needed to close this thing out. The goal is for Dan Griffin to have all the documents he needs to do a baseline submission towards the end of the month. Three to five documents make up the BOE: the accreditation letter, CAT report, test report, POA&M, and January 2009 UCDMO tick list. Larry Sampson will provide an updated template for the RM 5.0 fact sheet; the fact sheet is not part of the BOE, but will be distributed by UCDMO to the community.

Version 4 of the POA&M (commonly pronounced like 'poem') uses the following colour coding: dark green indicates findings that were fixed by a software change; light green indicates findings that were addressed by a procedural or configuration change (no software change); orange indicates findings that will be addressed by an immediate post-CT&E patch; blue indicates findings that have been deferred; grey indicates findings ruled invalid or out-of-scope. Charissa Robinson mentioned that her organisation plans to do multiple target-of-risk assessments: one for the CDS alone, one for the CDS with remote management, and so on, so that sites can use the one most appropriate to their situation. The pen test folks never did show up today. At the end of the meeting, Rob Drake noted that one of his Category III findings (non-critical) addresses a lot of 800-53 organisational controls---covering, for example, power supply sizing, environmental specifications, and so on---that have been left open by the current CT&E and ST&E procedures. These questions are not, in his experience, an ST&E event; they are a site event. Probably subsumed at STRATCOM by the existence of a SCIF and TEMPEST letter, at the moment they are still open, and need to be closed. It is all part of learning and debugging the new process.

There will be a hotwash telecon next week, probably Thursday. ST&E is completely done. A few housekeeping tasks remain, open action issues that are the accreditor's responsibility, but not of the developer, PMO, or the site. At present, 1st October 2010 is still being considered valid for a baseline announcement.

I have a meeting with Dr Martin tomorrow morning to talk about confirmation of status.

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

To be done immediately:

1. Work on the numerical model. Get an option mechanism (one-way) working. Code unit tests for bid/ask/post operations.
2. ACSAC submission deadline is two weeks away. I want to get the most recently rejected paper revised and submitted to this conference or to IM 2011.
3. Mr Ozura has been on an engagement and I have not been able to contact him yet; ping him again after Monday regarding Dan Nichols' refusal to contact. Try Frank Sinkular again. Dave Wallick should

```
be free now.  Try to get dates agreed for a late October or early
November trip.
4. Code the numerical model for risk--effort pricing equation.  Code
acid tests.  Find an equilibrium and fill in the blanks remaining
in the draft paper.
5. Meet with Dr Martin regarding confirmation of status.
6. Immediately after submitting to ACSAC, write draft confirmation
report.
7. Crosstalk article: immediately after writing confirmation report,
write the interpretation of the first case study in terms of
accreditor behaviour incentives.  Extend mnemonic anonymisation
codes and document them.  Write a preliminary overview of second
case study based on final reports from NSA I173 and I733 (from
memory; the reports themselves are classified).
8. Send out second group of US government accreditor surveys.  (What
went wrong the first time?) Look for UK government accreditor
names in old project records and get them in too.
9. Get the other two planned surveys done for background on the case
studies.
10. Make a fault-tree diagram for R-prime and S-star.
11. Draw up an org chart for R, R-prime, S-star, R-double-prime, N, L
and G.
12. Update anonymisation code chart (see above).
13. Finish methodology chapter (waiting on final survey questions).
14. Write first draft of confirmation report and send to Dr Martin.

To be done as soon as possible:

15. Update dissertation Table of Contents.
16. Collect examples of written work for confirmation evidence.
17. Compare NIST SP 800-53A to ISO 27001/2.
18. Update the schedule.
19. 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 0152.

References