File 20101112.0534: Weekly activity report 0162:

weekly activity report 162 (loughry)
Joe Loughry
Sent: 12 November 2010 05:34
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. 20101111.1454 (GMT-7) sequence no. 0162, week 5 MT

The SABI community is still holding their board meetings; RM 5.0 is
firmly on the UCDMO list, which is all that some managers care about,
but in fact there is a large difference between approved transfer
solutions that appear side by side on the UCDMO list, viz. RM and TMAN.
They are both on the list, but TMAN is TSABI-only and never will
be able to touch more than half the sites that RM in installed at;
nevertheless on the UCDMO baseline they look identical. Besides that,
even for a new listing, TMAN is hosted on an EOL operating system.
'It is a broken system' according to the developer; 'not even really
sure how they are on the list'. The SABI board has one more meeting in
November, but it will not be the last.

The programme office and UCDMO Technical Director (TD) exchanged
a series of emails this week that indicate they are serious about
streamlining the C&A process. The programme office is pushing to
include an incremental addition to the baseline technical capability
[email and Microsoft Office document files for USFK] and the UCDMO TD
wrote back that 'The CSTG RM Working Group was formed to facilitate the
development of a common body of evidence from CT&E and ST&E derived from
the first implementation of RM v5.0. This body of evidence would then
be available to support reciprocity across the DoD and IC.' He went
on to say, however, that the body of evidence is applicable only to
the first implementation configuration and architecture, i.e., the
UCDMO baseline, and any subsequent fielding of a CDS in other than the
baseline evaluated configuration would necessitate additional testing,
certification (if needed) and accreditation support from NSA and/or DIA.
The CSTG RM Working Group (CTSGRMWG) would not perform that additional
work; their mission is done [ref: 20101110.2221_RM_email_msg2].

The way I interpret this is that UCDMO-TD is wary of feature creep
and being asked to do 'just one more little thing' indefinitely.
The body of evidence as it exists at the end of the CTSGRMWG covers the
baseline operational capability and approximately four follow-ons (SNMP,
data link, remote management, RHR, and RHR-with-remote-management).
Email would be the fifth follow-on capability. The approval status of
the follow-on capabilities is still up in the air; CDTAB has slated TORAs
for the first four, but as of mid-November has only completed TORAs on
baseline, data-link and possibly SNMP. Other TORAs are planned to be
deliberated on in December. I have not heard yet of a TORA for the
email capability slated for deliberation by the board. Presumably,
either NSA I173 or UCDMO would update the body of evidence file to
contain the final determination of the CDTAB with respect to each of
the TORAs; that would bring the body of evidence up to date with the new
baseline---exclusive of SABI---and would make sense in the context of the
UCDMO list of approved solutions. I cannot say that this will actually be
done, however, especially in light of I173's busy schedule and funding,
which is not slacktacular. Dennis Bowden is contacting NSA regarding
the additional testing that IAD would have to perform for risk assessment
in service to the Army CDSO before USACDSO gives the packet to CDTAB or

DSAWG (DSAWG in the case of USFK) [ref: 20101110.2223_RM_email_msg4].

Some important organisational changes are imminent that will affect the inter-CDS-developer relations. At present, the RM developer is under Mr Bryan Rollins; TMAN is under Mike Warden, and because they fall under different umbrella organisations, TMAN has felt safe in the past to say bad things about RM. They do so constantly. The RM developer says they do not bad-mouth TMAN because the RM developer does not know enough about TMAN to feel confident in doing so. A planned reorganisation by Jim Quinn (LM VP) will likely soon place RM and TMAN under the same umbrella; that will make it much harder for TMAN to bash RM with impunity because the RM developer will be able immediately to respond. RM has a superior and more widely known reputation amongst prospective DoD and IC customers; TMAN is almost unknown in the collateral and IC community, being limited to DCGS.

The developer has a lot of installation activity going on for new TSABI sites and in preparation for initial SABI accreditations. Lots of hardware is being staged and the developer is porting to a new set of Crystal servers. These are MIL-SPEC-810F hardened for severe vibration environments, i.e., helicopter use. The developer is moving as rapidly as they can away from the current OS and hardware vendor towards an open architecture that will lower both cost and worry over hardware vendor product cycles---particularly the extremely distressing situation when certified OS product cycles get out of sync with evaluated configurations of available hardware. Related to the discussion in Augustine (1997, chapter 50), I read an interesting white paper this week, 'Using Time as an Independent Variable in the Determination of Appropriate Major Defense Acquisition Program Timeframes' (University of Tennessee Business School, 2010). In exactly the same way as was argued by Yegge in 2005 for software development projects at Amazon.com, this paper makes a case for controlling the cost of hardware and software development by fixing programme time lines before they can grow in cost. ('Cost as an Independent Variable' (CAIV) is complementary to 'Time as an Independent Variable' (TAIV) in this analysis.) The same idea was proposed in 1991 by Cordero, 1997 by Augustine, 2005 by Yegge and 2010 by NDBI under different Secretaries of Defence.

In other news related to my research, at the 4th UCDMO conference, the US government indicated how CDS developers should move away from Mandatory Access Control (MAC) to something new called Multi-Category Security (MCS). It is an extension of SE Linux atop the DAC and MAC extensions that hides some of the complexity of MAC from users. MCS is implemented in the security policy editor as a set of simplified MAC labels and roles. A new MCS translation service then runs as a helper between the kernel and the user's shell to control the visibility of files, processes and devices as the user changes roles, in a similar way to how MAC controls the visibility of files, processes and devices as the user changes security labels. It definitely looks like something CDS developers should pay attention to, although it is less directly applicable to an RM-type CDS than it would be to a user-centred CDS like TCS's Trusted Workstation. Speaking of which, Raytheon this week acquired Trusted Computer Solutions (TCS), a CDS vendor that is sort of in competition with the RM developer. TCS, in my experience, is a customised configuration of a CMW with Microsoft Office applications installed in the partitions and virtual network interfaces on the physical ports. It is something any end-user could configure out of spare parts, except that TCS have taken it through certification. However, a LAN of TCS-type workstations would be an ideal environment in which to implement MCS. I wish I had time to set up an MCS system and learn it, but I need to focus on my dissertation.

Dr Martin and I chatted for a bit on Wednesday via Skype. It was not a

formal meeting; Security Reading Group did not meet this week so I called to visit. I have not heard back from my assessors yet about a viva date for confirmation; I emailed Julie Sheppard to let her know that I need some lead time to buy plane tickets and the assessors might not be aware of that constraint; Dr Martin said he would send a note to Dr Flchais to let him know. It is not a problem if it stretches into December as long as I can avoid travelling near 25th November and Christmas, when the price of tickets goes up. Midway between those two dates, around 3rd or 4th December, travel costs are much lower than normal for the season. If I could get a viva scheduled for around then, I would jump at the chance.

I found a new tool that looks like it does exactly what I need: Simscape, an extension to Simulink, itself an extension to MATLAB. The makers do not offer a student licence, so I am trying to buy it directly. The tool allows direct modelling of physical systems with a numerical model that seems more suited to low-frequency, high amplitude motions than COMSOL, a vibration analysis tool that I also looked at because Lockheed has a licence for it. Dr Martin suggested trying to get an academic licence instead of a student licence. The academic cost is around 100, it looks like; if I can get that price I will grab it.

Dr Martin sent me a link to a BBC article about procedures for destroying the UK ID card database. We talked about that for a while, ranging into such other subjects as CCTV cameras and video storage. It is likely now that the MTBF of any new rotating-media disk drive will be reached before you are done filling it with streaming video at 15 fps; so who is keeping all that data? We talked about backscatter x-ray machines, the risk of radiation dosage and airport security. I get more exposure from the radioactive bricks in my house than I do from x-rays, although he pointed out that backscatter x-rays are interesting specifically because they do not penetrate---is the total dose absorbed in a few hundred microns of dermal thickness more than the bulk dose that would be expected? I ought to do some calculations on that and find out. I wonder if you can just buy dosimeters?

It's another thing I do not have time to chase down right now. We talked about creating a database of ideas for papers that no one has time to pursue at the moment. Some of them are timely ideas and ought to be explored, but if you are busy with immediate tasks and lack time to work on them, perhaps someone else could. For example, the idea I had earlier of a comparison of cost-per-experiment between the LHC, biotechnology, civil engineering (or materials) and software engineering. Certainly from CERN it ought to be possible to get accounting data down to the penny along with good data for the number of experiments, trials, PhDs generated (Dr Martin's idea) and papers published. I suspect it would be possible to learn some surprising things from a study of it. But I have no time to look at it now. We talked about carving out some space in the wiki (or elsewhere; the wiki is world-readable) for an exchange of ideas where anyone could deposit topics for new papers and other people could comment on them, or contribute, or just take an idea and run with it. Ideas could be tagged as in the Creative Commons system (Dr Martin's idea again) as freely available, or please-acknowledge-this, or I-want-co-authorship-and-half-the-Nobel-prize-money-if-this-goes-anywhere. Security researchers are a pretty competitive bunch, so I wonder how well this would be accepted. I am not aware of any similar systems with the possible exception of the Half-Bakery (not science-oriented) and an effort within Lockheed to get people to generate new ideas (also not quite the same thing). Students could use it as source of ideas for thesis projects. If I had time, I would make one.

We talked for a while about next week's Security Reading Group paper

on eScience, the Common Criteria, TCSEC/ITSEC, and why CMW was never adopted outside the defence community. I talked about how a teacher of mine once got undergraduates to read the literature for the first time ever by assigning the students every week the task of reading one classic paper from the literature and writing a one-page summary of it. He provided a list of classic papers if you knew of none, or you could bring him anything else. That was the best class ever; I plan to use the same technique some day.

I have been talking with Dr Stan Kladko at Aspect Labs, a CLEF in California that specialises in CC evaluation of high assurance systems. He is going to be in Colorado next week or the week after and we are arranging to meet at that time. He wants to talk about CC research and I want to talk about C&A in general and of improving the process from a software developer's perspective. It should be a good chance to get a parallel look at the problem, complementing what I can learn from the evaluators at CSC.

NIST released the 'On-Line Reference Database for NIST Special Publication 800-53 Security Controls' this week. It updates the security controls of Appendices F and G to the May 2010 set and cross-references to appropriate sections of SP 800-53A and the supplemental guidance (finally!).

Between trying to get Simscape purchased and working on the new outline for the Crosstalk article, I have been slowly finishing the annual report for Lockheed which is past due. I have a regular meeting with Dr Martin planned for tomorrow morning at 3:00 pm Oxford time.

My current task list (in priority order, most urgent first; work on tasks in this order):

1. Finish the yearly summary report for the Air Force.

2. Rework the Crosstalk article according to the latest thoughts. In the outline, I have that R-prime was evaluated under CC v3.0, but I recalled recently that there was an earlier version of that system (call it R_0) for the E project that was supposed to be 'evaluatable' under CCv2.3. R-double-prime was certified under DIACAP as the first test case to replace DCID 6/3, but it looks now like DoD and IC will be brought together by UCDMO soon, as soon as they acquire DSAWG control.

3. Thinking about what the definition of 'succeed' and 'fail' are in the context of CC evaluation: 'did not complete validation', 'abandoned before the end of validation', 'failed to receive certification', 'abandoned before the end of evaluation' and 'not submitted for evaluation' are all different and significant events.

4. Get a licence for Simscape and use it to modify the MATLAB simulation to do 4 systems in parallel with the same set of fixed points. Implement Prof. Polak's equilibrium acid test and the double alarm clock option model (should be easy to do in Simscape).

5. Background reading: Pennock and Wellman (2004) on uncertainty markets, Levitt and Dubner (2009) on asymmetric information, Bernstein (1996) on risk assessment (on hold), Karp (2009) on PhD research.

6. Ping the following people: Paul Ozura [BAH], Dennis Bowden [San Diego], [Patti Spicer, Charles Nightingale, Hal Forsberg at CSC], Dr Kladko [Aspect].

7. Small tasks: update first case study chart with changes from last

conference; draw fault-tree diagrams for R-prime, R-double-prime
and S-star; draw up organisation charts for R, R-prime, S-star,
R-double-prime, N, L and G; update documentation of the current set
of anonymisation codes.

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

End of WAR 0162.

References