File 20100806.0526: Weekly activity report 0148:

weekly activity report 148 (loughry)
Joe Loughry
Sent: 06 August 2010 05:26
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. 20100805.0934 (GMT-7) sequence no. 0148, week 8+7 TT

I have been studying background on microeconomics (anything related to
game theory) and risk transference. My copy of Gansler (1982) arrived
but I have not had a chance to get into it yet. Matlab is on hold until
I get to the book store for a student license. I have been catching
up on reading this week; digging into risk transference led to a lot
of articles on insurance. I am not sure how applicable that is to the
problem of accreditors transferring risk. I have been thinking about
a way of quantifying risk into transferred (or moved), mitigated (or
evaporated), and accepted (or booked) categories. If the quantitative
attribute of a risk is changed, that event may be due to work being done,
or promised to be done subject to verification, or because the risk has
been changed to a different category. If it is changed, that change
needs be communicated to all participants, possibly via a scoreboard.
The quantitative attribute of every risk affects, through summation, the
overall level of residual risk which may be different for each accreditor
but is an absolute value for the CDS. It is this relationship that
I am trying to explain for the extended version of the workshop paper
described below.

I am beginning to get replies back from accreditors around the IC and
DoD regarding meeting with them in mid October. The fiscal year ends
1st October which means US government offices tend to be busy in the
weeks beforehand, but after the first, budgets are sorted and I can get
appointments with these people. The Technical Director of the UCDMO is
first on my list. I am trying to schedule at least three appointments
in the D.C. and Maryland area during a stopover on my way to Oxford.
Nearly all are out attending the same meeting right now, but I should be
able to get something scheduled next week or the week after at the latest.
Then I will buy plane tickets for October. The ACM CCS workshop is
4--8 October; the beginning of Michaelmas term is 10th October; I will
plan to arrive in Oxford around the 15th (Friday) or the 18th (Monday).
I will ask Julie when I should submit paperwork for confirmation.

I contacted a friend in Space Systems to ask how they measure and
mitigate risks in flight hardware and software. There is a reference
in Harland and Lorenz (2005, p. 218) to a project that suffered from
heavy staff turnover---in particular, four Project Managers in just
over a year---that resulted in poor tracking of requirements to testing
and consequently doomed the payload (a scientific satellite) when
it was ultimately re-tested by the unforgiving environment of space.
The turnover in project managers is eerily similar to what happened to
R-prime; a number of other similarities are also apparent. My friend has
seen a few space vehicles built and launched; I described my model and
asked whether she could see any parallels. I want to understand more
about their approach to testing. On page 235 of Harland and Lorenz
(2005), an on-orbit failure is described; high-fidelity testing of a
real-time mission profile would likely have detected the software problem
that caused an over-long duration activation pulse to be applied to the
latching relay coils of STRV 1C and 1D, overheating them. Since that

event occurred in 2000, have they modified their testing philosophy? How does their testing philosophy compare to a CDS accreditor's, whose threat model is a heterogeneous group of human attackers vs the physical environment of space? The threat models are not un-analogous, I think. In both cases you have unexpected new threats that arrive asynchronously (via new attacks in the case of CDS,or newly discovered physical effects like bulk electrostatic charging in the case of spacecraft) and an attacker that probes incessantly for weakness. The space environment is not changing, with the exception of increasing orbital debris and consequent risk of collision, but the hardware sent into space continually changes with technology. I might be able to write a paper on that idea alone. Have to think about that.

Security Reading Group did not meet this week, but I sent editorial comments to Shamal about his new paper anyway. I have been catching up on reading this week. I bought a couple of books about risk and one on microeconomics, and I am re-reading some old books and highlighting relevant information. I received an email from a friend at Booz Allen Hamilton about their CCTL. He says NIAP CCEVS are now strictly adhering to the October 2009 policy that a government sponsor is required for evaluations above EAL 2. NIAP are redrafting protection profiles for COTS into seven 'technology communities' at EAL 2: (1) encryption, (2) network appliances, (3) laptop, (4) mobile (with the Trusted Computing Group), (5) PKI, (6) software running on Microsoft Windows (gets its own category!), and (7) server applications such as databases. Within a community, there might be modules, e.g., USB devices within the encryption PP.

Dr Martin and Dr Ashbourn might receive a call or email from the Academic Technology Approval Scheme (ATAS) related to my visa. I had to give them your names for referees, sorry.

Notification for the ACM CCS workshop is tomorrow. If my paper is not accepted, I plan to extend it and submit to the 26th ACSAC in December. The deadline for submissions is mid-September and the conference is in December.

I need to write my presentation and talk for the conference in Nice. I have an old IBM X30 I want to wipe and take along for email and presentation, avoiding carrying any critical hardware through either US or French customs. I have to give a talk at Lockheed next week on crypto maths; I need to prepare for that early next week.

RM 5.0 CT&E is complete. The developer received a copy of the final report from NSA I733 via USN SPAWARSYSCEN in Charleston. I read the report, which covers US government regression testing; penetration testing by NSA I173 will be reported separately. The report is classified. There were no surprises other than the way the report was written. The developer feels that the presentation of results was incomplete, resulting in an unbalanced impression to the reader. Every test that ever failed in regression was reported as FAIL, even things that were fixed during CT&E, re-tested, and passed. The developer intends to ask for an updated report that reflects the final findings; this should cut the immediately apparent number of failures down to a handful---some of which are actually 'the system is working as designed'---making the report easier to interpret. It is unlikely that any TOE will ever go before CDTAB with a completely green-light report; some of the security controls in 800-53 specified by a particular profile set are unlikely to be met in toto, if not actually found to conflict. I spoke with several of the developer's engineers about the report. I predict there is nothing in it that will prevent the STRATCOM accreditor from approving the ST&E on 20th August, but the report in its current state will give CDTAB and

DSAWG pause. I think the developer will get a certificate of some kind in August, but the first SABI sites are going to have a lot more work to do.

ST&E is reported to be under way and going well. Due to testing getting under way at STRATCOM, there was no telecon this week. Some of the participants will sit down at the UCDMO conference next week in Boston to discuss the progress of ST&E. I wish I could be in that meeting, but I had already decided not to go to the conference this year. I have asked people who will be in the meeting to report what happens, and I will try to obtain minutes. I am not sure whether next week's meeting is considered a formal meeting or an informal discussion.

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. Prepare talk for 13th August at Lockheed on crypto maths.
5. 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.
6. Accreditor surveys. I understand the problem much better now. I need to be able to describe these surveys in the Crosstalk paper.
7. Get the other two surveys done for background on the case studies.
8. Make a fault-tree diagram for R-prime and S-star.
9. Draw up an org chart for R-prime, S-star, and G.
10. Finish methodology chapter (waiting on final survey questions).
11. Write first draft of confirmation report and send to Dr Martin.

To be done as soon as possible:

12. Update dissertation Table of Contents.
13. For Chapter 3 or 4, start writing the interpretation of the first case study results and second case study preliminary results.
14. Compare NIST SP 800-53A to ISO 27001/2.
15. Update the schedule.
16. Apply for confirmation of status; submit written work.

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

End of WAR 0148.

References