File 20101002.0732: Weekly activity report 0156:

weekly activity report 156 (loughry)
Joe Loughry
Sent: 02 October 2010 07:32
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. 20100930.1348 (GMT+1) sequence no. 0156, week -1 MT

Important new events affecting my second case study and a new insight on the theoretical portion of my thesis prevented me finishing my confirmation report this week. On the other hand, I made significant research progress on two fronts. I will describe both in this report.

Last Friday, the RM 5.0 CT&E hotwash telecon discussed a surprising and disturbing report from the CDTAB meeting. Today, two final reports were issued from DIA and DNI. The UCDMO has not yet published the updated Baseline list of approved CDS applications, but it is expected imminently. The CDTAB threw a wrench into the process, however.

CDTAB met 21--22 September, after first inviting and then uninviting the developer and the Navy programme office. It yielded an extremely interesting second-hand account of shifting and conflicting personalities on the board. The day after the meeting, CT&E participants received a set of notes taken by Dana Pipkin [affiliation unknown], who attended the closed meeting and apparently experienced the proceedings as being sufficiently unusual to record her impressions of the personal interactions on display those two days. I got a call on Wednesday evening about the Pipkin report, and was able to view it on the high side on Friday.

Paraphrased, Charissa Robinson and her team from NSA were seen as very neutral, just providing the facts. Dave Oshman from NSA was also very neutral; he provided technical information only, with no opinions. Corinne Castanza (NSA pen tester) came across as an opponent to RM. She claimed to ‘almost’ have a technical attack working against the system, but left early before providing details and did not show up at all on the second day. ‘It appeared that her only intent was to drop her bomb and leave’, said Pipkin’s report.

Phyllis Lee and associate (pen testers) came across as distinct advocates for RM, providing technical information when asked. Editorial note: this is an historical role reversal between Charissa and Phyllis. Since the beginning of the CT&E telecons, Phyllis has always been the bte noir of RM, but at pre-CDTAB it was as if they had switched personalities.]

Glenn Learn was a neutral voice; he provided guidance on the Risk Decision Acceptance Criteria (RDAC). [Not to be confused with RBAC.] The CDTAB Chairman’s ‘statements would seem to imply that he was not a proponent.’ UCDMO representatives in attendance were generally neutral, not saying much.

The differences between service branch CDSOs were interesting. Dave Bowman of the Army CDSO was an advocate for the system and played the role of the voice of reason. The Marine CDSO representative was neutral and very quiet. Rick Perkins of the Air Force CDSO was clearly an opponent to RM, very vocal. Atri Amin and another SPAWAR tester, representatives of the Navy CDSO (and participants in the regular CT&E

hotwash telecons) ‘waffled between neutral and opponent to RM. At first they tried to stick to the test evidence, but over time jumped on the bandwagon with the other more vocal members of the board.’

A decision was made to divide the Technical Risk Review (TRR) into different TORAs (Target of Risk Assessment). Each TORA is one baseline architecture that is being evaluated by the board. It was explained that they did not want the risk rating for certain high-risk subsystems necessarily to affect the overall risk rating of the system. Last week’s TORA covered the generic guard functionality without any additional follow-ons. TORAs for Filter Strength Review (FSR), SNMP, WinDDS, Remote Management, and WinDDS with Remote Management will be held in October. The individual areas they looked at were in four categories, with the rolled-up results of each group determining (according to a table in the RDAC) the overall Technical Risk rating. The first category included network isolation, interface isolation, screening (this is where Corinne said she was ‘close’ and also where RBAC was discussed), and packet handling. The Category 1 roll-up was ‘moderate’.

Category 2 included process access control, trusted subject, least privilege and shared resources. The roll-up from Category 2 was ‘minimal’ which is not so good. Category 3 covers separation of account duties, account access control, and permission authentication. The roll-up was also ‘minimal’. Category 4 contained hardware architecture security, physical access control, software architecture security, least network functionality and configuration controls. The Category 4 roll-up was ‘moderate’. According to the chart in the RDAC, two moderates and two minimals roll up to a ‘High’ technical risk rating. [Editorial comment: ‘high’ technical risk is approximately in the middle of a five-element range. It is definitely not a show-stopper.]

Impressions from the CDTA board meeting itself: the board asked very technical questions, but barred the developer’s technical experts from attending. The board choose to rely completely on what the testers knew, but if testers did not know something, the board counted it against the guard. There are a few members of the board who are extremely vocal and negative, and the other members tend to go along with whatever they say. The board dislikes it when the developer or the government Programme Office decides, after due consideration, not to address a particular issue. The board interprets this as the developer not listening to the board’s feedback.

The board never takes into account findings fixed (and regression tested) during CT&E. If a thing was broken, then repaired, the board treats it as forever broken. The board consistently discounted recommendations in the DIA final report to close certain findings as having been addressed during CT&E. DIA’s opinion did not count in the eyes of the board. The board discounted anything that was done at site during ST&E, because those risk mitigations were not in the baseline as it was delivered to the site prior to ST&E. If it was not in the system at the beginning of CT&E, it was considered not to exist. No consideration was given to installation in a physically secure environment with cleared users (a very common explicit assumption in CDS security policies and CONOPs). The only thing considered was the evaluated configuration as it was delivered to CT&E. With regards to the OS version (RM 5.0 is the first version to be hosted on Solaris 10), the Pipkin report notes that the board did not take into consideration the fact that TSOL 8 has been EOL’ed by the manufacturer.

Pipkin’s narrative was of course discussed at the RM 5.0 CT&E hotwash telecon the following day. Before the meeting, a slide deck authored by Charissa Robinson (NSA Lead, CDS T&E) was sent out. It was titled 'Radiant Mercury 5.0 Joint Testing CT&E'; I wonder if this presentation was intended for CDTAB or somewhere else. It defined the following roles and responsibilities: UCDMO as the test coordinator/facilitator; DNI as Test Director and in charge of review; NSA for test review and penetration, of course; SPAWAR Atlantic (Charleston) are the test conductor; there is a defined IV&V testing team; and PMW 160 are the government programme management office. A brief history of the CT&E effort followed; the chronology agrees with my notes of each of these meetings.

[the following is paraphrased]

October 2009: NIST SP 800-53 controls vetted by community

18th November 2009: Test Readiness Review (TRR1) meeting

November 2009: IV&V (Alpha testing) at Lockheed Martin

4th January 2010: Security Design Review (SDR)

22nd January 2010: set of recommended 800-53 controls (approximately 600 in all) sent to community

8th March 2010: test procedures developed and sent to community

29th March 2010 through 23rd April 2010: CT&E (Beta testing) at SPAWAR

28th June 2010 through 23rd July 2010: CT&E regression testing at SPAWAR and pen test finding regression testing by I733

2nd through 13th Aug 2010: ST&E at USSTRATCOM WC RSC performed by DIA.

Quote: 'The Joint Test Approach (JTA) leveraged Alpha and IV&V testing. It incorporated lab-based testing to provide DoD evidentiary requirements and to perform potentially ''destructive'' tests. It accomplished Beta 2 and ST&E testing to satisfy IC requirements and DoD mitigation requirements. It was the prototype usage of 800-53 controls for CDS; will not ''certify'' in absence of 800-53a; used for test organisation and reporting understandable to the community. The controls will be tested to provide evidence necessary for utilisation by all communities. It will address additional NSA-submitted controls not yet adopted into 800-53 (i.e., Flow Enforcement).'

'Controls to Test Objectives will be a one-to-many relation. The results of ''certified'' evidence will be used by communities to assess control implementation in the context of their security accreditation.'

In particular, the slide deck quoted NIST SP 800-37, a useful definition of CT&E and ST&E: 'Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. [Source: NIST SP 800-37]' [citation in original]

The following testing evidence comprised the Body of Evidence (BOE) presented to the CDTAB: Alpha/IV&V testing report, POA&M Validation Report, CT&E report with regression testing results from SPAWAR with

I173 oversight, I733 penetration testing, and the Beta 2 ST&E report from DNI/CAT. (Source: ‘Radiant Mercury 5.0 Joint Testing CT&E’ by Charissa Robinson. Undated, unclassified//FOUO.)

In light of the Pipkin report, the RM 5.0 CT&E hotwash telecon on 24th September was better attended than most. Present on the call were Kevin Miller, Russ Savage, Joe Loughry, Larry Brown, Craig Christensen, Kori Phillips, Larry Sampson, Mia ?, Orville Brown, Kevin Gallicchio, Dennis Bowden, Dave Oshman (NSA), Charissa Robinson, Atri Amin and Corinne Castanza. Rob Drake was missing. The CDTAB on 21--22 September decided to discuss only the first of six TORAs (Target of Risk Assessment) that are planned to be reviewed. Neither the developer nor the RM PMO have seen the first TORA yet; it should be sent through the low-side email soon, probably Monday when Amy Arroyo gets back.

There were four sections in the TORA; as described, a ‘high’ technical risk rating on any two triggers a ‘high’ rating for the entire CDS. [Editorial comment: the range extends all the way up to ‘extreme’ at the highest end.]

The board wanted the Technical Risk report shared with the developer and the government Programme Office. Dan Griffin is unhappy with the ‘high’ technical risk rating; he wanted to know if there would be an opportunity to rebut. Atri explained that historically, the rating stays where it is, unless there was some serious error. It would be necessary to request another review to have a chance of getting the rating changed.

Kevin Miller put the rating in perspective. RM 4.0.5 received a ‘high’ rating, which did not slow down adoption of that version. RM 4.5, with new capabilities, inexplicably received a ‘medium’ rating. The ‘high’ technical risk rating of RM 5.0 suggests that the CDTAB rating process is inconsistent at best. The board specifically requested some additional ST&E tests that they would like to see run. [Editorial note: this is relevant to Larry Brown’s observation that members of the CDTAB are migratory, like CDS installers; they spend a lot of time on the road, you rarely see the same group of people twice, and the results of your ticket depend a lot on the luck of the draw, what members you happen to get when the CDTAB meets that particular month.]

Corinne, Atri and IV&V were with Charissa in the CDTAB meeting. Dana Pipkin later sent her email to Charissa. The board asked for the developer to submit their ticket now.

Dan Griffin asked, ‘So now, with this high technical risk rating, how is this going to play with SABI?’ If RM PMO wants to get the risk rating changed, it will be necessary to use the Navy CDMO for leverage. The developer is not permitted to contact the board directly; the developer must go through the Navy CDMO, which goes to the board, and the board then contacts Atri’s people to perform additional testing and modify the BOE. Only the board can contact Atri’s people. I173 needs to have a ticket before they can work on anything.

Dan Griffin asked about bringing additional evidence to the board. I173 responded by requesting that RM PMO provide the missing evidence so it can be included in the BOE provided to CDTAB and the Community Jury. Developers are not permitted to put evidence directly before the board; the developer must give the evidence to I173 through the Navy CDMO.

Lots of systems get a ‘high’ technical risk rating. It is not a bad rating. I173 would be very surprised if the rating changed.

Corinne then amplified for the telecon participants on her remarks during CDTAB that she was close to having a viable attack. There are too many of the default Solaris components left in; the OS was not stripped enough. DNI and NSA agree on that much. They are also not happy that the guard crashed several times at STRATCOM; they did not expect to see stability issues this late in the CT&E.

The next telecon will discuss whether a Version 5 POA&M is needed; the board's recommended additional ST&E procedures will go in any updated POA&M and must be added to the ST&E plan for DoD sites.

Larry Sampson said there would be a CD-CSTG meeting on 30th September. A number of briefings are slated, on the new risk management framework, RM 5.0 CT&E, and talking about moving forward with the CSTG. He next brought up the issue of closing down the RM 5.0 testing effort. Dan Griffin noted that the only thing left to do is the response to the pre-CDTAB report.

The IC risk assessment is still to come. Need to keep going with these telecons for the time being. They can wrap up in October. The 19th or 20th of October is when CDTAB meets again. Dan Griffin once again asked for a knowledgeable technical expert (developer software engineer) to be standing by outside the room where CDTAB meets, this time to answer questions in support of IV&V representatives who would be inside the room. UCDMO again said they would consider it. [Editorial comment: last time they said that, they changed their minds at the last minute and denied it.]

Dennis Bowden asked if Rob Drake is still on track to provide an accreditation letter by 30th September. Kevin Miller asked at what point will RM 5.0 be on the UCDMO baseline. Pending triage of the CDTAB report, pending everyone sending in their final reports, and pending one ATO from either DoD or IC, it will be on the next published list. Atri reported that the lab has expended all their funds; nothing is left to support any more testing. There is barely enough for one more trip to attend.

After the telecon ended, the developers discussed the call. Larry Brown expressed concern that a 'high' technical risk rating will necessitate provision of screening routers and anti-virus at sites; Russ Savage commented that none of that helps the RBAC problem anyway. Craig Christensen said he is worried that if sites see two solutions, one with a 'medium' risk and one with a 'high' risk then the site will choose the one that has a lower risk on the tin; Larry and Russ countered that after the initial period when a product is first introduced, no one looks at the risk rating. Like a person's undergraduate grade point average, for the evaluation of an experienced candidate it will be forgotten, Craig asked, can we get through the initial period? Russ pointed out that for SEW, JCDX and shipboard duties, nothing else but RM can do the job. A five-way technical discussion of alternatives for addressing the RBAC issue followed.

Meeting adjourned to Craig Christensen's office at 10:00. Larry Brown advocated for a 5.1, 5.2, 5.3 release schedule every six months; get them disseminated so that customers start demanding the 5.1 capabilities. Every six months a new one is released; maybe only every third version gets certified.

At 10:00 the developer called Dennis Bowden regarding the patch question. Engineering sees nothing in the patch as it currently exists that addresses any of the CDTAB concerns; the developer wants to redirect patch testing effort to focus on the new issues. By pushing the patch out to a later date (call it 5.01) an improved patch could take care of more of the issues important to the CDTAB.

Dennis Bowden: nobody, not CDTAB nor UCDMO are pushing for a patch. The next significant activity, and a significant expense, is the test event for the current patch. Delay the test event, and a single later test can cover a better patch, without requiring a second test event to take place.

Dan Griffin: we should wait for the reports to arrive on Monday.

Kevin Miller: remember, the October TORA reports will come out afterwards. Suggest we hold off the entire test event until those other TORA reports come out. They will likely generate new issues.

Dan Griffin: I am not ready to do that. I want to have the 5.01 patch available in case UCDMO says RM 5.0 cannot field without it. We will wait until Monday and meet formally again then.

There followed a discussion of what to do next. The developer attempted by means of engineering arguments to convince RM PMO that the October TORAs will almost certainly generate new CRs. In addition to those, it would be advantageous to address Corinne's issues. The developer recommended strongly to push all of those back from now into a single, better patch and test it once.

Dan Griffin: I am still concerned that UCDMO might come out and say RM 5.0 cannot field without this small patch. RM PMO is willing to pay for a second test event for a larger patch if and when it becomes a necessity (which is likely). The meeting finally adjourned with RM PMO unconvinced.

The developer believes that the deck was stacked against them during this CT&E. NSA I173 contracts out regression testing to Fort Huachuca and SPAWAR in Charleston, and this time it was Charleston's turn. It was the first time Charleston had ever seen Solaris, so they were unfamiliar with it, and wrote a lot of findings that show their poor understanding of the OS. The developer expressed frustration with certifiers who won't read what the developer writes. In addition, many findings have been duplicates; when the developer responded in writing with a clear explanation of the error, the certifiers apparently did not read the responses and continued to report the same nonsensical results and conclusions. The latest report is that the RM PMO requested in the strongest terms a re-evaluation of the CDTAB's technical risk rating. The response from UCDMO was 'you can send it to us'. That is not encouraging in the developer's view.

[Editorial comment: based on what I heard directly from participants and attendees who were at the CDTAB meeting, I think the developer ought not to request a re-review. The chances of getting a different result seem to me to be close to zero. The developer should instead work on their pitch to be used with prospective customers to the effect that a 'high' technical risk rating means the product has a lot of powerful capabilities (which is true) and hence comes with a 'high' risk rating the same way a sharp knife does. TMAN, as a point of contrast, side-stepped the issue a while ago by abandoning the entire SABI process and settling for TSABI accreditations only. They no longer have to put up with CDTAB. Other CDS developers have taken the same low road, by purposely limiting the capability of their products and avoiding the difficult certifications.]

The developer expressed some more frustration at the lack of a leader throughout the CT&E process; there is no one in charge, only a committee. There are no mandatory attendance requirements at meetings; important participants sometimes do not show up for weeks on end. Because participants represent different agencies, there is no coherent chain of command.

The developer finally talked the Programme Office out of spending any more time on the minimal post-5.0 patch that had been planned until CDTAB uncovered the ‘high’ technical risk rating. The CDTAB report illuminated the reasons for several mystifying CT&E findings. The developer now feels that the first post-5.0 patch must be larger to include certain specific functionality. The developer successfully argued for a much more comprehensive post-5.0 patch that might not be issued until six months after the first systems were fielded.

In the RM 5.0 CT&E hotwash this morning, on 1st October, the participants were supposed to discuss Version 5 of the POA&M, but most of the government people said they had not received it yet. The stated agenda of the meeting was to discuss Corinne’s and Charissa’s final reports.

Present on the call were Larry Sampson, Kevin Miller, Joe Loughry, Craig Christensen, Dennis Bowden, J. somebody for USSTRATCOM Western Region, Dave Oshman (NSA), Don Flint, Orville Brown, Charissa Robinson, and Corinne Castanza. Dan Griffin was away because of a death in his family; Dennis Bowden represented the government Programme Office today.

Dennis Bowden started off by saying that he is waiting for an accreditation letter from Dan (?) as soon as he gets back from travel. The accreditation letter, formal evidence of an existing ATO at the SABI or TSABI level anywhere, is a required component of the Phase III ticket exit criteria.

Version 5 of the POA&M includes all DIA, DNI and CDTAB concerns. As was discussed by some of the government participants at CSTG last week, the POA&M is intended to be a living document, updated with new information about threats and mitigations as they are developed over the years that a CDS remains in operational use. Speaking for Dan Griffin, Dennis Bowden stated that the 5.01 patch will contain fixes for all findings identified in the POA&M as requiring a non-procedural mitigation. It will be necessary for LM and RM PMO together to spend the next few weeks determining what regression tests are required, as well as what kinds of testing will be required from external agencies. Early next week, Dennis Bowden will talk with Dan Griffin and the developer about it.

The developer is working with an excellent new document written by Corinne that explains the RBAC problem. It will take several weeks to make all the necessary changes, but the effort is under way already. Corinne praised the developer for being so proactive.

Dennis Bowden said there are four customers that really need 5.0 right away. He asked if it would be possible to work with the CDSOs to get those four sites briefed at the October CDTAB, as the operational need is urgent. Charissa said she met with Paul Ozura earlier in the week; she asked if those sites have Phase I tickets in place. Answer: yes; all that is needed is the Cross Domain Appendix to complete Phase II. As soon as that arrives, they will proceed to Phase III. CDA template is done now. Charissa asked whether the four customers are upgrades or new installations. Answer: they are all new installations. Dave Oshman stated that it is really the CDSOs that need to push in order to get those sites slated for CDTAB.

Orville Brown and Corinne discussed a technical question about the label_encodings and exec_attr files in the POA&M. The upshot of it was that if certain capabilities are operationally necessary, then they are, and Corinne will simply have to document the risk assessment on them. She is OK with that as long as it is documented.

Larry Sampson then said that from the UCDMO perspective, until the mid-October time frame, the participants will leave it open to have as-needed classified or unclassified telecons. Corinne noted that feedback from NSA I173 is that they will have their final pen test report by November. Dennis Bowden asked, as you prepare to brief the next CDTAB, please consider inviting IV&V. He talked with Glenn Learn at CSTG last week, and understands now better why the developers are not let in.

Call ended 08:30. After hanging up, the developers again discussed the call amongst themselves. Kevin expressed frustration that ‘they never read anything we send’. Ian noted that ‘ninety-five percent of the government people claimed never to have received the Version 5 POA&M. Don blew Corinne’s cover when he said ‘‘it’s in the folder’’.’

Kevin said Corinne wrote a great paper on the RBAC problem. He noted that the proposed solution will necessitate more telephone support time; every time the site wants to debug it will be necessary to change the user_attr file and reboot; this will take a good engineer at least thirty minutes extra on the phone. They are considering adding a button to do it, but from Corinne’s perspective, that is another attack vector.

The UCDMO Baseline List was not published today (1st October), but that is not surprising; sometimes it takes them a few days. It is on the unclas internet; I am watching for its appearance.

In a classified email this week containing a document titled ‘Major Findings out of the CDTAB TRR for feedback to RM PMO’, it was noted that in the context of the next TORAs that (U) ‘follow-on capabilities will drive open the system’s data risk’. [Editorial note: the preceding sentence was portion marked Unclassified.]

Two important final reports were published this week. The first was ‘Defence Intelligence Agency (DIA) Security Assessment Report (SAR) for Radiant Mercury Version 5.0 Baseline’, dated 14 September 2010, S//NF (DIA, 2010). This report is the first to state that DIA performed ST&E of RM 5.0 at USSTRATCOM, Western CONUS Regional Service Centre (WC RSC) Omaha, Nebraska 2--13 August 2010 in an unclassified portion marked paragraph; it was the first operational installation of RM 5.0, and serves as both an operational and a Baseline ST&E event. The event validated mitigations of findings from CT&E.

The following quotation from the report will be useful later on:

\begin{quotation}
(U) The purpose of the ST&E was to demonstrate that sufficient procedural and automated safeguards have been implemented within the system to permit the system to process the Top Secret information in an operational environment at Offutt AFB, Omaha, NE. Specifically, the objective of security certification testing is to show that Radiant Mercury operates with an acceptable level of risk as required by National and DoD standards. That is, to show that Radiant Mercury:

a. satisfies operational requirements

b. provides required user identification and authentication.

c. provides required discretionary access control on files, application, and hosts.

d. provides sufficient restrictions on access to security sensitive files.

e. provides the capability to retrieve and display audit trail records.

f. confirms that procedures for site backup, continuity of operations, and emergency destruction exist, if necessary.

g. confirms that methods for site configuration management exist.
\end{quotation}

This is also the first place I have found in writing that states that ST&E test procedures were originally created using DCID 6/3 requirements; following discussions amongst DIA, DNI, DoD, UCDMO and RM PMO, it was decided that RM 5.0 would instead go through the NIST C&A process instead of DCID 6/3. 'ST&E was followed by a comprehensive penetration test event by the DNI Certification, Accreditation and Test (CAT) Team.'

At the end of the report, 'The following recommendations have been provided:' [paraphrased]

a. 'the Test Director recommends RM 5.0 be granted a Baseline
        Accreditation Letter.'

b. [it is] to receive an ATO with POA&M for STRATCOM for three years.

The second final report to be issued this week, by the Office of the Director of National Intelligence, United States of America, was 'System Assessment Test Report for Radiant Mercury (RM) System Version 5.0', version 1.0, dated 2 September 2010, prepared by the IC CIO/ICIA CAT Team (DNI, 2010). This report states that the ODNI IC CIO Intelligence Community Information Assurance (ICIA) CAT Team performed penetration testing on the RM 5.0 system, in operational service at USSTRATCOM, WC RSC, Omaha, Nebraska from 16--20 August 2010. Assistance from the STRATCOM Red Team in assessing Top Secret collateral and SIPRNet network infrastructures was acknowledged.

Finally, I learnt from the metadata on the report that Corinne Castanza is with IC CIO/ICIA CAT Team; she works for Calleen Torch, DNI/IC CIO/ICIA/CAT Chief.

After all that, I went back and reviewed Burton (1993) on Pentagon procurement policies. It's been a long week. There was no stop-work order, as had been feared last week; it was only NMSO playing their usual games with funding. They came through with the money at 17:05 local time on the last day of the contract period.

At the same time all this was going on, I had an insight on the risk market problem at the centre of my thesis. I invented the risk market idea after running into difficulty getting accreditors in the US and UK to talk to me; it seemed wise to activate Plan B when the second half of my planned research (an ethnographic study of accreditor behaviour by means of surveys) seemed to be getting nowhere. If I had a numerical simulation, I reasoned, then I could perform experiments on it and compare the results to observed accreditor behaviour, of which I have plenty of examples from my first and second case studies. Even if the accreditor surveys did not pan out (and I have not given up on that yet), I would have another theoretical component available to write about in my dissertation. Along the way, I proved an interesting result in economics, which led credence to the belief that my artificial model of accreditor behaviour was viable. It is more complicated than the usual case of CDS accreditation, true, but I claim that my model is just complicated enough to encompass both intra-national multi-agency and international CDS accreditations, an important special case applicable to Radiant Mercury, if not other CDS systems.

The problem was, although I could describe the characteristics of the model in abstract terms, I could not implement it. I figured out a solution on 25th September, and successfully implemented it in Simulink (a MATLAB library) the following day. In the present embodiment, accreditors are fixed points on a surface. For reasons to be explained later, the surface has a non-zero coefficient of friction. The accreditors' position on the surface is defined within a Cartesian coordinate system of risk tolerance vs the relative influence that the accreditor has on the CDS vendor, site, and certifiers vis- -vis other accreditors. Risks are interpreted as multi-tonne masses sliding on the surface, mass proportional to the amount of work (expressed in test procedures performed and witnessed by IV&V) needed to mitigate the risk. Bids in the risk market look like springs, or rubber bands, connecting an accreditor with a risk. Bids exert a force, based on the spring constant and frictional damping, through a vector that acts to move the risk in the direction that the accreditor wants it to move. If a particular risk is already where the accreditor wants it to be, there is no reason to make a bid. There is no energy input to the system, so it must converge. [I need a reference for that assertion.] Accreditors who join after CT&E may cause dynamic readjustments; for example, with new coalition partners in a dynamic coalition CDS. I implemented this in Simulink and immediately observed risks moving in the direction I expected them to move, towards an equilibrium at the lowest potential energy level. I worried, however, that---not being an expert with MATLAB---I might be fooling myself. To check this, I constructed a physical model to validate the MATLAB simulation. Screen door springs and nails hammered into a board last weekend showed good agreement with my second-order MATLAB model (second-order meaning that it models not just the spring constant but also damping from friction). The breadboard model showed definite differences in how it behaves, because it is not damped very well. When the pin holding a risk in the initial position (established by the CT&E baseline) is released, the risk orbits rapidly the final position before settling down after a few seconds. That behaviour is not well shown by the MATLAB model yet. I also do not know how to plot the motion graphically yet, but I will, after I get my confirmation report written.

There are a number of physical motions and constants in this model that I have not figured what they correspond to yet. What does the initial position really signify? What does the final position signify? Of what significance is the path that a risk takes on the way to equilibrium? If the mass of a risk is the time-integrated amount of work needed to mitigate or at least completely characterise it, it takes a while for inertial masses to move. What does that mean? These are all questions that need to be answered. I still don't know what options mean in this model. Rubber bands with alarm clocks attached?

Dr Martin asked me to write the confirmation report from a risk management perspective. I think I can characterise the risks now, and provide a convincing mitigation plan for each. If Dr Ivan Flchais is to be one of my assessors, I should follow the advice he gave me once: always point out the flaws in your own solution. If Dr Jirotka is to be my other assessor, I had better have a good explanation ready for why those US and UK accreditors wouldn't talk to me. With a physics-based analogue in hand, I am less worried now that the risk market approach might not work. In fact, I think it has interesting implications for

Covert Channel Analysis (CCA), the most pernicious problem in all of CDS development and accreditation. If the CCA problem in CDS could be solved, that would be a real breakthrough.

The above explanation will be cut and pasted into my confirmation report. I will get it written as soon as I finish the DARPA proposal for Lockheed, which I need to do before Monday.

The COMLAB-CS-2010 programme committee met on Friday to assign submissions to reviewers. I took papers on security, software engineering, graphics and linguistics. I have seven papers to review.

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

0. Write DARPA RFI response for Lockheed (this weekend).

1. Confirmation report is past due to Dr Martin.

2. Email Dennis Bowden with my standard set of questions.

3. Finish the Pennock and Wellman (2004) tutorial on uncertainty markets (long).

4. Submit forms for confirmation of status to Julie.

5. Get a date set for telecon with Patti Spicer, Charles Nightingale and Hal Forsberg at CSC.

6. Quarterly progress report and FY 2010 summary progress report for the Air Force; write a new introduction for DARPA based on the last two years' work.

7. Implement an option mechanism based on the Dutch pattern; implement 'acid test' as unit test.

8. Appendices A--C of the confirmation report.

9. Finish reading Augustine (1997).

10. Small tasks: update first case study chart with audience suggestions from VALID 2010 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.

11. Got a reply back from Paul Ozura; waiting for more.

12. Crosstalk article: immediately after writing confirmation report, write the interpretation of the first case study in terms of accreditor behaviour incentives; write a preliminary overview of second case study based on final reports from NSA I173 and I733, DNI CAT, ST&E, POA&M Validation Report, and CDTAB.

13. Based on what I learn from Paul Ozura, rework the other two planned surveys done for background on the case studies.

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

End of WAR 0156.

References