File 20101015.0603: Weekly activity report 0158:

```
weekly activity report 158 (loughry)
Joe Loughry
Sent: 15 October 2010 06:03
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. 20101014.1127 (GMT-7) sequence no. 0158, week 1 MT

Julie Sheppard emailed me yesterday to ask where my Confirmation forms
are.  That was my fault; my supervisor and I have been discussing it
for weeks but I forgot that the forms were supposed to be submitted in
noughth week, not first week.  I contacted Julie immediately and said I
will get the forms to her right away.  The GSO.14 form asks for several
different narratives on progress and direction that I can pull from
historical GSS reports.  I will have the forms done tomorrow.

I am still trying to find time to finish the MATLAB model of the 2D
dynamics simulation.  I want to put the resulting phase space plot
(showing how the interpretation of it matches observations) in my
confirmation report.  As described in reports 156--7, I think that the
concept of a critically damped system is inapplicable to the accreditation
interpretation; rather, the system behaves as if it were underdamped.
It implies certain qualities of motion of risk assessments that have
been observed in practice and leads to a new hypothesis: that the
time evolution of a multilateral accreditation may be related somehow
to simple harmonic oscillation.  If the damping coefficient exists,
it must be (a) small and (b) related somehow to the amount of work
that an accreditor must do, measured (as before) in person-hours.
I need a formula to convert person-hours to work packages or test
procedures-completed-and-signed-off; in the real world people have
different fully burdened cost factors, but in my model I treat them as
individual parameters forced to 1.0 for simplicity.  Later on, if I want
to use the tool to predict actual costs, I can fill in realistic values
and scale the output.

This week was hopeless for making progress beyond the first chapter of
the Engineering Mechanics Dynamics book (Harper, 2007).  I am treating my
problem as two separate calculations harnessed together: motion on the
$x-axis$ is independent of motion on the $y$-axis except that both are
updated in lock-step.  On the subject of Risk, I have been thinking about
differences in the way economists categorise risk versus the way engineers
do.  'One of the fundamental underpinnings of the financial world is
the concept that the greater the risk in an investment, the greater the
return.' (Augustine, 1997, p. 134).  Does this have any interpretation
with respect to risk in accreditation?  Accreditors receive no return
on investment from accepting responsibility for the residual risk of an
operational CDS (other than experience which tends to improve their risk
assessment skill in future).  Data owners receive a return of increased
functionality in return for the risk they accept.  CDS developers and
installers receive their return in the form of an increase in trust for
their CDS, leading to a reduction in accreditor $k$-value for future
accreditations.  But does an increase in risk lead to greater returns?
In the case of CDS developers, it does.  In the case of data owners,
I believe functionality may be orthogonal or at least only tangentially
related to risk.  For accreditors, I think there is a weak correlation.

These are all topics that need to be worked out in my dissertation.
```

To get there, I have to convince two assessors that my plan for accomplishing it in the next year is viable. Here is my planned TOC for the dissertation:

Chapter 1: Introduction to the problem of CDS accreditation and CT&E.

This chapter will lay out the characteristics of cross domain systems and what makes them different from conventional security certification test and evaluation problems. Why they are different from safety-critical systems and the criteria used to test and evaluate those. History of computer security test and evaluation standards. Current standards applicable in DoD and the Intelligence Community (IC). What are the roles and responsibilities in different types of CT&E and ST&E across the defence and intelligence communities of the US and UK. Comparison with the Common Criteria.

Chapter 2: Literature survey

From Trithemius through the Elizabethans and to Wilkins, who faithfully documented everything that had come before; the long drought through the first World War and into the second; realisation by several governments that military computer security would soon become an important problem; development of the first military standards. Evolution and cross-pollination of those standards. Safety critical standards. Adoption in the commercial world: ISO 17799/27001. Independent development of parallel standards; attempts and failures at harmonising different books. The Common Criteria. TCSEC, ITSEC, DITSCAP, DIACAP, NIACAP. DCID 6/3 and its predecessors. NRO C&A standards. NIST Special Publications 800-37 and 800-53A. The future of non-military security C&A.

Chapter 3: Methodology

This chapter will introduce two case studies and an abstract model of intra- and inter-national CDS security accreditation for the CT&E and ST&E phases of tactical operational CDS installations. A catalogue of available documentation for each case study will be described. Specific parallels will be drawn to US and UK government security standards to show that the configuration of the model is necessary and sufficient to mimic all important events observed in both case studies. A discussion of rejected alternatives will explain why certain other approaches (an ethnomethodological study of accreditor behaviour and attitudes, in particular) were not chosen. Economic interpretation of the model. Physical analogue of the model; theory and design of the MATLAB simulation of time-varying parameters of the physical analogue; validation of physical analogue An interpretation of each physical parameter in the numerical simulation and how they are assigned to accreditation decisions and events. Pre-selection of confidence intervals for tests of statistical significance. Policy and procedures for handling proprietary, classified, export controlled and personal information.

Chapter 4: Evidence

The precise sequence of events in each case study will be determined. Ranges of allowed values will be determined from observations according to the methodology. Numerical simulations will be run over the domain of allowed values for each of the independent variables in the physical analogue.

Chapter 5: Interpretation

Comparison of the available evidence for both case studies: identification

of gaps in the information and exploration of reasons for the missing information. Comparison with the coverage provided by simulation results. Evaluation of the fidelity of the simulation against observations. Analysis of the reason behind any differences between simulation and observations. Statistical significance.

Chapter 6: Summary and conclusion

Plans for making changes to the model to improve prediction value. Plans for elaboration of the model to include cost and schedule forecasting of accreditation efforts. Five-year plan for future work: development of tools to support IC CDS accreditation. List of available CDS development projects against which tools can be validated.

Appendices

A. Deanonymisation codes for case studies

B. Proprietary, classified and personal information appendix

Security Reading Group met Wednesday this week to go over the paper 'Privacy and Security for Online Social Networks: Challenges and Opportunities' by Zhang, et al. (IEEE Network, 2010). The paper was suggested by Cornelius. There were only a few people in attendance but we had a good discussion on security and privacy design goals. Issues around Facebook's privacy settings are well known, but a new and interesting invisible privacy opening in Facebook is the implicit relationship that game players have with software providers and advertisers. Farmville players see the explicit relationship with a named set of their friends in the game, but not visible to them are connections between Zynga, the third-party software company that runs the game, and fourth-party advertisers who, arguably, are Zynga's real customers. Game players' attention spans are the product sold by Zynga to its consumers (advertisers), who are shielded by a level of indirection through Zynga from directly being limited by Facebook's privacy settings, privacy policy, or auditing.

In the middle there was a lively discussion on the acceptability of citing Wikipedia in a scholarly article. Most were against it, noting the temporal variability and vulnerability to sabotage that are characteristic of Wikipedia articles. I noted the existence of the change log and suggested as a possible compromise that if a Wikipedia article must be cited, it should include the date and time (reckoned to GMT and precise to one second) when the article was retrieved. This is similar to the usage in Wikipedia's Policies and Guidelines for referencing web pages in Wikipedia itself, although the Policies and Guidelines permits only the date of retrieval; that is not precise enough in the event of an edit war. The audit log for Wikipedia changes is displayed only to the minute, although 1 second precision can be found by decoding the URI of log entries. In general, though, everyone in Reading Group expressed a dislike of finding Wikipedia anywhere in the reference list of an archival paper.

Ronald Kainda brought up the authors' multiple overloaded definitions of 'personal space' on page 14 of the paper. He did not like the term, feeling that it was unclear and poorly defined. We experimented with my webcam image on Skype to try to measure whether the feeling of personal space extends across a video teleconference link, and decided that no, the remote person is still 'miles away'. But is it true that comments

written by others are part of your personal space? Comments written by a second party can affect the way you are perceived by a third party on LinkedIn, necessitating regular monitoring of the graffiti on your personal space in every social network you have ever signed up for.

We discussed the low-level implementation of social networks and the implications of single point of failure. As the authors point out, users see the top level of network topology and may have a very different impression of nodes and edges than are realistically or reliably supported by the logical and physical topologies beneath. Could it be possible to design a social network from good security principles bottom-up, rather than trying (as Facebook had to---messily---a year or so ago) to retrofit security to a legacy infrastructure that was not designed for it? Dating networks are a fascinating special case that was not mentioned in the paper: at least three people in Reading Group hit on this realisation simultaneously. Dating site operators have a strong incentive to distribute as widely as possible a carefully limited amount of information about nodes, but the operator loses exclusivity if viewers can aggregate enough data to deduce a connection without going through the network. Real estate listings are another---different but related---example of the problem.

I want to suggest for next week's Reading Group the paper by Gelman and Stern, called 'The Difference Between ''Significant'' and ''Not Significant'' is not Itself Statistically Significant' [The American Statistician 60(4), pp. 328--331, November, 2006]. I put it up on the wiki.

Lockheed demanded a block of continuous time this week on a combination of the DARPA-SN-10-73 RFI proposal and the annual performance review cycle. The proposal was submitted to DARPA before the deadline. I am hopeful that it will provide my next couple of years of funding. The DARPA proposal is based on the success of the AFRL research project begun in 2008 and asks DARPA to fund the development of a multi-user declassification tool as a follow-on to Tom Marso's successful prototype. I currently owe the Air Force two reports for Q4 of Phase II and FY 2010. These are on stop-work order whilst a funding problem with the sponsor is worked out.

I wrote seven reviews of submissions for the COMLAB-CS-2010 conference and uploaded them on EasyChair in time for the deadline. The programme committee will meet this week to sort the reviews and select approximately 50--60% of the papers for presentation at the conference. In all, we managed to get 76 reviews written of 31 submissions for 15--20 slots; I am going to recommend that my paper be rejected because I will probably not be in town to attend the conference.

The Oxford University Scientific Society (OUSS) has a full programme of evening lectures slated this term; I updated the web site and calendar for the society's term card and have been discussing with Colin Murphy how to record the lectures and make them available as podcasts on the Pulse Project web site.

The UK Consulate sent me an email advising me not to purchase any plane tickets until they have physically given me my passport back. Not sure what's up with that.

The UCDMO has still not updated the Baseline list of approved CDS but an announcement was made this morning that something called Trusted Manager has been placed on the UCDMO baseline. In a conversation earlier this week with a member of the RM 5.0 developer's organisation,

it was mentioned that a new chief technical person in the IS&GS division of Lockheed Martin wants to have one guarding solution, and it's not TMAN or RM. This new entity might be the one he was talking about. The press release was scarce on details but the RM 5.0 developer is preparing for a fight to justify continued funding for the existence of three different CDS products within the company. RM and TMAN, we know, are suited for different jobs; Trusted Manager is an unknown quantity but it seems to have high-level executive support and a certain amount of credibility in the community, given that (they claim) it will appear on the next UCDMO baseline. I forwarded the press release to the RM 5.0 programme manager to find out if he knew about it. RM 5.0 is not owned by Lockheed; the rights are owned by the US Navy; Lockheed owns the crucial technology at the centre of it. RM 5.0 has in hand a TSABI accreditation letter but the SABI accreditation letter must wait for the first accredited installation of a SABI system; several customers are taking RM 5.0 sites before the DSAWG in December, after which those installations will go operational and a SABI accreditation letter will be issued. By that time the remaining TORAs will have been completed by CDTAB in October and UCDMO will update the RM 5.0 baseline with the rest of the follow-on capabilities. I learnt another piece of UCDMO information this week but it is not for redistribution. When events make the information public then I will be able to talk about it.

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

1. GSO.14 and MAT.3 forms completed and delivered to Dr Martin for signature; ask Julie Sheppard to forward the forms to St Cross College next.

2. Confirmation report.

3. Get the 2D model working reliably. Generate a reasonable looking phase space plot.

4. Contact Dennis Bowden; follow up with Paul Ozura.

5. Finish the Pennock and Wellman (2004) tutorial on uncertainty markets (deferred from last week).

6. Submit final written work to department.

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

8. Quarterly progress report and FY 2010 summary progress report for the Air Force (on hold until next week for funding)

9. COMLAB-CS-2010 committee meeting; arrange for server space to host podcasts for next OUSS lecture.

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

11. 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.

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 0158.

References