File 20100924.0644: Weekly activity report 0155:

```
weekly activity report 155 (loughry)
Joe Loughry
Sent: 24 September 2010 06:44
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. 20100923.2010 (GMT+1) sequence no. 0155, week -2 MT

I met with Dr Martin today briefly to talk about confirmation of status.
Earlier in the week I had to pick a date to give to the immigration
authorities for my next travel to the UK; I chose 11th November for the
purposes of making the visa application.  I emailed Dr Martin to ask
whether it would be possible to schedule a confirmation viva around
that date.  Everything depends, of course, on the availability of
assessors, including time for assessors to be selected and to read the
confirmation report and consider the evidence.  I have not made travel
arrangements yet, so the dates from my perspective are totally flexible.
We talked about the possibility of attempting to do a viva through Skype,
but I said I would prefer to come back to Oxford and do the viva in
the traditional way.  I have an immigration interview next Wednesday to
obtain the required biometrics identity card for re-entry to the UK.

We discussed how confirmation of status dates work.  I believe I need
to submit the necessary forms by end of First Week, and complete the
viva by the end of Michaelmas term (effectively, then, by the end of
this calendar year).  It is currently Week 0-2.  Dr Martin told me it
is acceptable to submit evidence separately from the forms; therefore
I should get the forms to him for signature right away.  I will send my
draft confirmation report to Dr Martin tomorrow.

We talked about selection of assessors.  For my transfer report, Dr
Simpson and Dr Jirotka were the assessors; this time, Dr Simpson is on
sabbatical so this time it may be Dr Ivan Flchais and Dr Jirotka again.
Dr Martin will talk to the assessors and see who is willing.  On the
question of evidence, I am eager to get the viva done as soon as possible,
but Dr Martin advised that it is better to push the date back and have
more evidence to show the assessors than to try to do it earlier with
less evidence.  The real deadline for the viva is noughth week of Hilary
term, but I will check with Julie and get the forms submitted now.

Today I gave a talk to an audience of Red Team and Blue Team security
engineers at Lockheed Martin on penetration testing techniques,
specifically emanations security attack and defence modes.  The audience
were located in Orlando, Florida and Bethesda, Maryland.  The job of
this group is to perform internal penetration testing and security
improvement on code and systems used for corporate operations and
unclassified aerospace development (such as the F-35 Joint Strike Fighter)
and systems integration contracts.  They were interested in low-cost
attacks that would be directly transferable to Blue Team operations.
I described the range of new research results in this area since the year
2000, pointing out connections when applicable to published reports from
1948--1985, and looking in some detail at low-cost attacks such as the
one by Barisani et al. (2009).  Questions afterwards included defence
against and detection of malicious hardware; for example, counterfeit
Cisco route processors compromised at the factory by means of chip-level
modifications.  I discussed the conclusion of some branches of DoD with
respect to this problem; because of the lack of a TPM in that hardware and
```

the difficulty of physical inspection, the response DoD eventually decided upon was to log absolutely all traffic with ubiquitous IDS sensors, giving them the capability, at least, of forensic analysis later on to spot the covert channels that they suspect might be in the devices.

Some interest has been expressed from DARPA this week in another project I am working on. Several people think that the recent RFI for DARPA-SN-10-73 (New Technologies to Support Declassification) is a close fit to some work I started in 2008. Currently that work is funded by the Air Force on a three-year contract; DARPA may want to pick up the tab for development past FY 2011.

Books: I am trying a new book on MATLAB. Currently I am extremely frustrated by my inability to get the numerical model of accreditor--accreditor interactions working reliably. I have also started reading Augustine's 1997 book which was recommended to me for the author's insight into the problems that developers face working for the U.S. government. I have a copy of the Port Royal Logic (in translation) on order.

The Comlab DPhil Student Conference programme committee meets tomorrow morning to divide up papers amongst the reviewers. The conference received 31 submissions this year, a significant increase over last time. The problem now is finding enough reviewers to minimise the number of papers each reviewer has to read. We are trying to reduce that number from eight papers each to no more than three. One of the submissions is mine; EasyChair has a conflict detection feature that we will try using tomorrow in the committee meeting.

The regular RM 5.0 CT&E hotwash telecon will occur on Friday, not Thursday this week. I will be there; the participants are expected to go over the final POA&M and results from the pre-CDTAB that took place on 21st September. I received some second- and third-hand reports from the pre-CDTAB meeting that indicate it was a very interesting gathering, different in many ways from the official version of what CDTAB is for, who the various members are, and how they are supposed to interact. I will have a chance tomorrow to read a first-hand report from the pre-CDTAB session; I have not seen the report yet and do not wish to pass on unsubstantiated rumours. I will relate the results of tomorrow's telecon and yesterday's participant narrative from the 21st in next week's report.

New results: I am waiting for a reply from Paul Ozura; in response to his earlier email, I sent back a detailed description of what I am trying to accomplish through contacting US and UK government accreditors, quoting examples of the queries I have used and responses I have received so far. Mr Ozura offered to help try to open some of the closed doors I am encountering on a regular basis. The telecon with CSC evaluators in the CLEF has not been set up yet; I am waiting for Mr Nightingale and Mr Forsberg to return from travel. In Bernstein (1996, p. 112), the author says 'If the satisfaction to be derived from each successive increase in wealth is smaller than the satisfaction derived from the previous increase in wealth, then the DISutility caused by a loss will always exceed the positive utility provided by a gain of equal size' [emphasis in original]. I think this provides an explanation for Schneier's observation from 2008 that people tend to fear a loss more than they value a gain in a trade. Books on risk analysis that were written by economists necessarily are geared towards monetary examples; books on risk written for the safety and security community are slanted in an orthogonal but not quite useful yet (for my purposes) direction. I keep having to interpret to my problem domain. For example, the difference between the Port Royal Logic and Bernoulli's 'New Theory'

is not unlike the difference in risk outlook that stands between US and UK accreditors: Bernstein characterises Arnauld (1662) as saying ‘only the pathologically risk-averse make choices based on the consequences without regard to the probability involved’---which sounds just like NSA with its risk-management policy. Bernoulli, on the other hand, asserts that ‘only the foolhardy make choices based on the probability of an outcome without regard to its consequences’---which again sounds just like CESG accreditors I have known, reflecting an institutional policy leaning more towards risk avoidance where possible. CESG frustrates the Americans, just as NSA’s apparent recklessness often appals the British. [Source: Bernstein (1996, p. 100 et seq.).] I believe I can apply this to accreditor behaviour incentives in a generalisable scenario. Based on a metric I defined for total residual risk, the risk market should allow me to enable semantically limited and covert-channel--free ad hoc communication amongst DAAs participating in a single CDS accreditation. The cost of a risk is set by the data owner affected by that risk; the price of a risk mitigation is proportional to an amount of work (e.g., test procedures completed and witnessed) that must be done by someone---but not necessarily the bidder---for the accreditation to proceed. By formalising signals, I hope that an efficient route to agreement about the true level of residual risk in a CDS accreditation will avoid repeated re-testing and redundant risk mitigations. The preceding is what I am presently attempting to describe in a paper, now titled ‘An Artificial Risk Market Solution to the Problem of Information Asymmetry in Cross Domain Systems Security Test and Evaluation’.

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

1. Draft confirmation report due to Dr Martin tomorrow.

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

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

4. Submit forms for confirmation of status to Julie.

5. 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.

6. Trying a new MATLAB book; keep trying to get the numerical model working again.

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. Wednesday: interview with immigration authorities.

12. Waiting for reply from Paul Ozura.

13. 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.

14. 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 0155.

# References