File 20101104.2024: Weekly activity report 0161:

```
weekly activity report 161 (loughry)
Joe Loughry
Sent: 04 November 2010 20:24
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. 20101104.1003 (GMT-6) sequence no. 0161, week 4 MT

Trying to track down a reference last weekend, I ran into an example of
what librarians call a black hole or a dark age: periods of history that
are not accessible due to changing technology.  The document I was looking
for is called either 'Government Procurement' or 'Govt. Procurement' and
contains hearings before the Senate Select Committee on Small Business,
85th Congress, 1st session, from either January or March 1957.  The call
number is Y 4.Sm 1/2:P94/8/957.  But when I went to that room in the
regional depository library, all I found were pieces of shelving on
the floor.  The microform collection is being digitised and decades of
microfilm are unavailable.  It will have to wait until the next time I
am in Washington and can look for it at the Library of Congress.

My confirmation report and written work have been submitted to the
department.  Dr Martin's suggestions were incorporated; I explained
how the written work fits into the structure of the thesis, provided
a more complete TOC of the dissertation and provided word-counts where
appropriate to give an indication of how much of chapters 1--3 have been
written so far.  The report is a little longer than department procedures
require but I felt it was important to give sufficient background and
context.  I am looking forward to a date for the viva; I need time to
schedule plane tickets.  (I will go the Library of Congress in D.C. on
the way to Oxford.)

The Unified Cross Domain Management Office on Friday issued a
new 'Baseline List of Solutions Available for Re-Use' with several
interesting changes appearing for the first time.  RM 5.0 was listed with
no qualifications in the Transfer category.  'RM 4.x.x and all previous
versions' appeared in the list of 'Sunset' solutions to be retired out of
inventory no later than 31st October 2012 in accordance with the November
2009 CRDB.  This marks a significant advance for the RM developer.
As reported last week, TORAs for baseline and data link were completed
by CDTAB in October but TORAs for SNMP, remote management and reliable
human review in combinations will not be completed until end of December.
From the Programme Office perspective, the UCDMO baseline list is all that
matters, as that is where data owners and DAAs will look when specifying
and accrediting new installations.  The new baseline version is 3.6.0.

Finishing the Air Force Research Lab (AFRL) quarterly report for Lockheed
plus revising the confirmation report took up a significant chunk of
time last week; I am currently finishing up the AFRL summary report for
FY 2010, which turned out to be a larger job than I expected.  I hope to
have it done by tomorrow.  As soon as it is delivered, I will work on the
Crosstalk journal article some more.  AFRL requested a demonstration of
the probabilistic redaction technology on 15th November at their UCDMO
conference to be held in Rome, New York; I will not be at that meeting
but will get notes from it.

I have been handling OUCS registration renewal for the Oxford University
Scientific Society's mailing list and web site this week; updates to
```

the web site are pending. I have a request from Jackie Wang to look at a research proposal; I need to contact the person.

The Security Reading Group met Wednesday to discuss the paper by Lee and Yu (2009) titled 'Towards a Dynamic and Composite Model of Trust' (SACMAT '09, June 3--5, Stresa, Italy, 2009). Anbang introduced the paper. Cornelius asked me about Enomaly, a company that recently announced a trusted cloud provider mechanism called ECP High Assurance Edition. How it is implemented is not clear from the marketing material, but it is said to be based on Intel TXT and TPM to perform remote attestation. Nice to see it in a commercial product. If it takes off, cloud providers may succeed in establishing their own definition for the term 'high assurance platform' that is different from the military usage. I will be interested to see if they attempt Common Criteria evaluation.

In the paper, the authors begin with a definition of vertical and horizontal trust, something that several participants in Reading Group had a quarrel with. The distinction between horizontal and vertical credentials is fuzzy. I think the authors split it in two for the purpose of having two kinds of credentials to feed back into the composition operation later, so they could show the closure property working. Their motivating scenarios were useful, although it would have been more useful if the exact same scenarios has been carried through from Section 3.1 into Figure 2 instead of a slightly different variation; it made the notation more difficult to follow. The five requirements in Section 3.2 added little, although I thought the authors' explanation of the closure property and roles/policies in Section 4 was clear. Their notation for RT_0 and the parametrised variant RT_1 was missing sufficient definition of what some of the things are. A digital certificate is a credential, as Dr Martin observed, but in order to use it you usually do a proof-of-possession protocol, signing it with a private key. But the protocol is not the credential. The authors used a notation $2^\mathcal{F}$ for the power set of $\mathcal{F}$ that I had never encountered before, but it makes sense if you think of the binary expansion as a combinatorics selection. Also, I think the reputation score f still works if you clamp the results to 0 or 1, thereby reducing a horizontal reputation score to the equivalent of a simple vertical all-or-nothing credential. Neat.

Cornelius remains unconvinced of the correctness of the authors' method. There was a long discussion of sequential composition and whether the proposal in the paper really solved it, or whether conjunction and disjunction alone are sufficient. I think there is a semantic difference between 'a reputation score of at least 0.85, as reported by members of the ACM' and 'a reputation score of at least 0.85, and $\mathit{output} > 0.85$' but Cornelius is not so sure. I believe that sequential composition is needed, although I am not sure about linking containment.

I liked the paper more as I got nearer the end of it. The technical features and considerations in Section 5.3 seemed to me to have some useful applications, and the authors were careful to point out where their model breaks down in the presence of incomplete information or communications interruption. The comparison with RBAC in Section 6 was good and should be pulled out and put into a review paper. Several portions of this paper would make a good contribution in the form of a review paper. Dr Martin asked the question 'what can be done after reading this paper that couldn't be done before?' I think the method in the paper is a start, but it is missing too many needed tunables to be implementable as it stands. I hope other researchers pick up CTM and improve it rather than inventing something else. The method, although flawed, I think has potential to be refined into a useful model.

```
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 latest thoughts.  Produce a
detailed outline and write introduction ASAP.

3. Reading.

4. Modify the MATLAB simulation to simulate 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.

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

6. Ping the following people: Paul Ozura, Dennis Bowden, Patti Spicer,
Charles Nightingale, Hal Forsberg. [not done yet]

7. Email to Jackie Wang.

8. 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 0161.

References