File 20100122.0230: Weekly activity report 0120:

```
weekly activity report 120 (loughry)
Joe Loughry
Sent: 22 January 2010 02:30
To: Niki.Trigoni@comlab.ox.ac.uk; Andrew Martin; Joanna Ashbourn
Cc: andrea@hpwtdogmom.org; Joe Loughry; mmcauliffesl@comcast.net
Attachments:
Weekly activity report no. 20100121.1816 (GMT-7) sequence no. 0120, week 1 HT

Dr Martin pointed out this morning a new report from the European
Network and Information Security Agency (ENISA) on Cloud Computing Risk
Assessment.  The report was most interesting to me for its description
of the risk assessment process they used.  Risk assessment is crucial
to the tool I have to develop later this year.  I am reading the report
more for insight into its methodology and techniques than anything else.
I think there are at least two techniques I can use from it (see below).

Reading group started up again this week with a presentation by
Shamal of his and Ivan's new paper on a meta-model for usable security.
Shamal has three publications now so I'm feeling the pressure to keep up.
The methodology chapter outline is developing well and is on-track for
completion of the writing in another 2 or 3 weeks.  That, combined with
a re-purposed version of the poster I made for ACSAC 25 that was not
accepted last December, will make a good paper for the journal Crosstalk.
I plan to submit that paper by the beginning of March.

We met formally twice this week to talk about my methodology chapter
outline.  I included it with the agenda each time to show how the chapter
is evolving.  Besides commenting on the organisation of the chapter
(in particular suggesting how I could make clearer the relationship
between pieces of the methodology) and on my writing style, Dr Martin
gave me more advice on research, writing, and presentation.  I have added
a survey of subject matter experts (SME) on the relationship between
testing effort and the principle of defence in depth to the methodology.
I think this will provide a useful perspective that is orthogonal to
the recollections of participants in the first case study and the second
case study.  Finally, I am still looking in the security-critical systems
literature in case anyone has found a set of axioms or theorems that
would seem to be adaptable to answering the question I have, which is:
how much testing is enough?  How do you know when you're done?

On Monday, Dr Martin questioned the connection I want to draw between the
well-established principle of defence in depth and the level of testing
that exists in people's minds---whether that connection really exists.
We talked about it back and forth for a while, and about the way it
relates to formal methods, and about process depth as compared to
test depth.  Dr Martin pulled a few books off the shelf behind him and
suggested Leveson (1995) as a possible source.  If the axioms I am looking
for don't appear in that textbook, he said, they probably do not exist.
I got a copy from Amazon yesterday.  The safety critical literature has
its own fundamental principle: ALARP (As Low As Reasonably Possible)
which is found throughout the field, especially in chemical engineering
and process plant operation.  Dr Martin reminded me to look in the SCS
course notes, which I had forgotten about.  I found a long paper by
Bowen and Stavridou (1993) that might have a pointer in it.

In Thursday's meeting, we talked more about the safety literature and my
expanded outline.  Dr Martin advised me not to lose momentum writing by
reading too much in the security literature this week.  Focus instead
on writing and expand the outline into prose.  To reiterate, the plan
```

```
is to have this chapter completely written by 19th February when I give
a talk on it before the department.  I am on a roll and want to keep
that momentum.  Lockheed is still a problem; I am trying to push back
and keep them from demanding more of my time than is fair.

Tasks:
1. methodology chapter
2. Software Engineering talk (19th Feb)
3. Crosstalk article (to be submitted by 1st March)

Reading:
1. ENISA report (for their risk assessment process and SME survey methodology)
2. Leveson (1995) looking for security-critical axioms or theorems I can adapt
3. Probably not Anderson (2007)

Next meeting: Thursday, 28th January at 1400 Oxford time.

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

End of WAR 0120.

References