

File 20090409.1230: Notes from meeting with Dr Martin today:
From today's Weekly Activity Report (WAR):

From: Joe Loughry joe.loughry@stx.ox.ac.uk
To: Andrew Martin sabbatical@andrewmartin.name, Joanna Ashbourn joanna.ashbourn@stx.ox.ac.uk, Niki Trigoni Niki.Trigoni@comlab.ox.ac.uk
CC: Andrea Loughry andrea@hpwtdogmom.org, Joe Loughry joe.loughry@stx.ox.ac.uk
Date: Thu, 09 Apr 2009 22:30:58 +0100

Weekly activity report no. 20090409.2217 (GMT+1) sequence no. 0079, week -2 TT

I met with Dr Martin today for an hour in his office. We talked about Trust 2009 and some of the contacts with people that I made during the conference. In particular I spoke with Professor Cynthia Irvine of the Naval Postgraduate School; she was one of the authors of the Separation Kernel Protection Profile (SKPP) and a valuable source of information related to my thesis. I also met David Kleidermacher, CTO of Green Hills Software, also highly relevant to my research.

One of the things Dr Martin and I discussed today was how many data points I need to prove (or disprove) my hypothesis. So far I have only one—clearly not enough, but the SKPP and the successful evaluation of INTEGRITY at EAL6+ are two more data points that I can get access to with fair ease.

I think I made a good impression on Prof Irvine; she pointed me to an old technical report (136 pages) of which I was not aware, and I followed up after our conversation with an email. I also followed up on my conversation with Mr Kleidermacher of Green Hills Software, in which I seriously suggested that a book needs to be written about their experience. It could be written as a cracking adventure story, like Tracy Kidder did in *The Soul of a New Machine* and Richard Rhodes did with *The Making of the Atomic Bomb*. Both of those were very good books. Mr Kleidermacher in turn (perhaps jokingly) told me I should write it. I've been thinking about that, and today I discussed it with Dr Martin. I don't really have time for another project right now. But Dr Martin asked me whether the necessary research for that book—at least in the early stages—might not be relevant to my thesis. Dr Martin suggested I should follow-up with Green Hills Software and request access, under the auspices of academic research. I immediately sent a carefully worded email to Mr Kleidermacher. He hasn't responded yet but he's probably still travelling.

Dr Martin and I also talked about the practice in Chemistry of staking a claim in print to a particular area of research, and whether it might be a good idea to do something like that in my case. Not to preclude being scooped, but to bring other potential sources of information out of the woodwork who might then contact me. We talked about the best sort of journal to do that in, and talked about getting the Security Reading Group to have a discussion of what the best journals and conferences are currently in this field.

Dr Martin suggested an interesting short paper topic, relevant to my research: a comparison of CVE reports to Common Criteria evaluated products—is there a correlation? Finally we talked about college and department support for fieldwork and travel to conferences. Prof Irvine strongly suggested that I get to the International Common Criteria Conference, which she said is always held in exotic and expensive locations. I'm going to look at past proceedings of those conferences for now.

Next week we will not have our regular meeting so that I might concentrate on studying for the ISSEP exam.

Upcoming deadlines and events:

- 10th April: Good Friday
- 12th April: Easter Sunday
- 17th April: submission deadline for 2009 NSPW
- 24th April: St Cross College tour of Stonehenge

- 25th April: ISSEP exam, London
- 26th April: Trinity term begins
- 28–30 April: Radiant Mercury User’s Group (RMUG) meeting
- 30th April: Infosec show (all day) in London; I am helping out

—

Joe Loughry

Doctoral student in the Computing Laboratory

St Cross College, Oxford

How many data points do I need? Obviously, one is not enough. Two are good for curve fitting. Three are great if you already know what direction you want the curve to point. (‘If you can choose the three points’, said Dr Martin.)

Use Green Hills as a positive example. Use RTG 1.0 as a negative example. Use SKPP and HASK-PP as examples of PP evaluation. Use INTEGRITY-178b as a positive example. That’s five data points!

Get different people’s perspectives: PP writers’ perspective, vendors, NIAP, CESC.

Staking a claim is the norm in Chemistry. It could be useful to stake a claim here because it would announce it to the world and other people that I might never have heard of otherwise might contact me. It could bring previously unavailable sources out of the woodwork.

Pairwise Analysis: show some table listings: how the failure did it, compared (in the next column) with how the successful ones did it.

Short (easy) paper idea: correlation of number of vulnerabilities in CVE *vs* EAL? Question: has the CC shown its worth yet? Could be a short paper. WIP at a conference, maybe.

When I publish a conference paper, the University gets some prestige. The department, and my college, probably offer support for getting to the conference if I am reading a paper there.

Colleges sometimes pay for fieldwork. I’m doing fieldwork in the US!

I think Dr Martin was a bit more pleased with my progress this week. Happy Easter!

References