File 20100113.0729: Notes from meeting with Dr Martin:

Started off by mentioning the GSS report. Has Prof. Kwiatkowska responded yet? No, the system notifies us both when she reads the report, and she probably hasn't read it yet.

For Prof. Kwiatkowska, if I do end up talking with her, I want to be able to show two things (n.b. not three—see the notes from my meeting with Steve Steinberger on 20100110). Firstly, to show that I have progress. Secondly, to show that I have a roadmap.

Next we looked at my methodology outline (attached to the agenda). I said I need help with the thesis statement. Dr Martin agreed that I don't really have a problem (in the quotation on page 1 of the agenda) but then asked me to say in five or six sentences what my 'problem' is. I did. He told me that's a pretty good thesis right there. I was surprised and pleased to hear that from him.

I mentioned that I am getting excited again because this is such a cool technical problem that I really want to know the answer to. I remember Dr Martin telling me things two years ago that I made notes of at the time, and I remember him telling me then, but the same things make a different kind of sense to me now, after I have gone down all the different blind alleys that I did. In short, I am thinking about the same things differently now than I did when I started.

Dr Martin looked at the beginning of my methodology outline and asked what is the objective? Make it more clear from the beginning of my methodology narrative just why I am doing these two case studies. I think I was figuring to put the objective at the end. Dr Martin asked how it recursively decomposes.

What is the objective of the steps in the methodology?

I mentioned that I feel it needs a bit more theory. What is the controlling theory behind security CT&E? I asked for any ideas he might have of where to look for one: in a related field, perhaps. Dr Martin suggested two things: firstly, what is the common theory behind the CC, for example? Is it to make software better? Insurable? To reduce the attack surface? To CYA?

Another parallel might be in ISO 9001 certification.

You also might be able to find something like theorems or axioms in the safety literature.

I wonder if there is any theory. If there isn't one, I may need to think of one. Question: what have others done? What theories from other fields might I be able to adapt?

With my five or six sentences newly discovered, Dr Martin asked me to look at theses in the Comlab library (note: do this in February when I'm there on Saturday and Sunday) for their thesis statements. You will find that they are not well formed, usually.

Another idea for finding a theoretical basis for my thesis: search for criticism of the CC or notes for improvement.

I had the idea (whilst talking to Dr Martin just now) that people confuse the duplicated effort in CT&E with the principle of defence in depth.

Dr Martin: the safety literature is a good place to look.

Here are my five or six sentences on the problem. Email this to Dr Martin in a few minutes: (note: this is done)

> It is widely acknowledged that information security Certification Test and Evaluation (CT&E) is expensive in terms of time, number of people required, and duplicated effort. That high cost makes CT&E a special event that is not done often, either because fewer systems requiring CT&E are made, or because not all of them are tested, or because the ones that are made are tested less often. Defence in depth is a well-established principle of infosec engineering, but people confuse the duplication of effort in CT&E with defence in depth. The massive overexpediture of time and effort does not yield an attendant increase in security.

I saw an article just yesterday criticising the idea of defence in depth (in the context of IDS and antivirus) as being obsolete because the way we should think of data is not in terms of files, but as mobile information that is where we need it when we need it, and not there at other times.

On a roll, so I am not going to take any time to update the schedule just yet. Striving to complete the methodology chapter ASAP.

Next meeting is scheduled for *Monday* 18th January at 0700 MST.

References