File 20100519.0700: Notes from Reading Group this morning:

I presented my paper 'Unsteady Ground: Certification to Unstable Criteria'.

I wrote this short paper for the purpose of introducing an audience to the background of CDS since there aren't any—or hardly any—conferences in my subfield (not a lot of literature either). One of the problems with that situation is you spend a lot of time on background, and I am really constrained by the page limit here.

I am working on a related idea that characterises the residual risk accepted by accreditor A which might be different from the residual risk acceptable to accreditor B because whilst both probably agree on the set of threats it is desirable to mitigate, they might have different clearances, and hence know about different sets of risk mitigations, at least partly disjoint. (Not correct use of the word 'partly'.)

Presentation Tip: don't talk about 'accreditors' before explaining what an 'accreditor' is. The audience hasn't read the paper yet. Your talk at the conference is to *convince* people to go read your paper!

In the context of CDS, I mentioned the paper by [1] and made the claim that modern cars are Cross Domain Systems.

Cornelius said that in Section II, I really have two problems, not one. You first talk about ST&E, but then give two examples of CT&E, and then you're talking about ST&E again. It's confusing.

I talked about reducing the number of rounds of ST&E after a system is CT&E'd from 1000 down to around 10.

John asked whether the tool is intended to collate evidence from previous accreditations? Answer: yes. The idea is never to have to run the same test, on the same equipment, with the same connections, by the same people, using the same test procedures, more than once. The accreditors may be different.

Cornelius asked if my problem is still too big. I agreed, saying that when I go to Confirmation of Status in a few months, the assessors might look at this and say it's still too big. You have two different problems here, and to Cornelius they look nicely separable. The historical study of two CT&Es, one unsuccessful and one successful, plus the thesis question of 'is there a difference in post-CT&E software defect rates...' is one problem, and the development of a tool to minimise re-work in ST&E by collating and sharing accreditor information is another problem. There is plenty of room for future work here, probably five years worth. It will keep me busy for a long time.

Cornelius suggests picking one or the other: CT&E or ST&E for the DPhil.

Notes on the Introduction (and this agrees with the reviewer comments from the conference):

John suggests showing at the beginning the similarities between the two examples, then talk about differences. As it stands, it looks like two completely different systems, when in fact they're the same software. John and Cornelius both: how are the two examples related?

How is CT&E similar to ST&E?

The final camera-ready copy is due in two days. I have to finish the talk for Lockheed first, then get some sleep, then hit this paper hard to finish and get it re-submitted before Friday. Sleep first now until about 09:30 a.m.

Call ended 0645.

References

[1] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage. Experimental security analysis of a modern automobile. In *IEEE Symposium on Security & Privacy*, Oakland, California, 16–19 May 2010.