File 20091028.0636: Notes from meeting with Dr Martin this morning:

- It was lucky that I started an hour early this morning, because it took that long to get Skype working. The webcam, for some reason this morning refused to show video. Skype reported only 'Unknown Error'. Audio was working, for once. But the camera refused to work. Re-installing the driver didn't seem to help, but eventually downloading a new driver, re-installing the driver, un-installing the driver, blue screen, re-installing the driver, and rebooting a few more times than seemed necessary and for no apparent reason, it started to work again. I do not know if it will work reliably the next time I connect, so for now I'm going to leave it alone and hope it keeps working long enough to get through this call. Next week, be sure to get up early again in case we have to go through all this Mickey Mouse again.
- I presented at Reading Group this morning, the paper 'Security Through Information Risk Management' [1].
- My thoughts: it is easy to measure threats; it is hard to measure risks.
- Quote from Ivan: 'risk is the probability of a measurable loss.'
- Does this paper have any conclusions? No. But I think it will be cited in future as a useful snapshot of CIOs' opinions about information security risk in 2009.
- Next week's reading group might do one of the two papers on empirical methods in software engineering ([3] or [2]) as a way of balancing the current paper.
- Dr Martin: [1] is very US-centric. It would be interesting to see another paper like this with a more European perspective.
- Regular weekly meeting with Dr Martin started at 0800:
  - It's light outside the window now. It won't be next week at this time.
  - I apologised for not having the *Crosstalk* article done. Dr Martin noted that I owed it to him last Friday.
  - I told about writing the Summary Progress Report for Probabilistic Redaction the last few days. I wrote a three page report, it was sent back with 'insufficient technical detail' and I had to rewrite it as a 13-page report. It is never good to have a report sent back as unacceptable. I had a bad week.
  - 'That happens', said Dr Martin.
  - I need to fix on milestones and meeting milestones in order to maintain progress. Dr Martin again cautioned about the importance of maintaining progress.
  - I talked about the RM 5.0 CT&E testing that begins next week. It is an exciting opportunity to observe CT&E testing of a large system from the beginning. This is a particularly interesting case because it's the first time both the developer and the certifier have worked with the security controls of SP 800-53. It is a completely new C&A standard. I will be in the kick-off meeting on Monday when I will get to meet the Certifier face-to-face and be involved from the beginning in this testing. I am trying very hard not to get left out. A lot of it is politics, talking to people, and trying to get included and not left out.
  - This CT&E testing will be a valuable new data point for my thesis, and good for validating the tool I'm developing on an actual CT&E testing of a major update of an existing system by a certifier and a developer both of whom are experienced but neither of whom have worked with this new C&A regime before.
  - I lamented that I'm not very good at estimating. I need to get better at that. You estimate something as well as you can and it still takes three times longer than you think it would.
  - Now that the Prob. Redaction report is out of the way, I want to go back to writing the *Crosstalk* paper. I will have that for Dr Martin for our next meeting on Wednesday.
  - Now task: go back to work on the *Crosstalk* article.

  - We talked a bit about time zones, DST, BST and GMT and UCT.
  - Next meeting: Wednesday, 4th November after Reading Group.
  - Dr Martin says, 'work hard'.
- Call ended 0817.

References

[1] M. Eric Johnson, Eric Goetz, and Shari Lawrence Pfleeger. Security through information risk management. *IEEE Security & Privacy*, 7(3):45–52, July/August 2009.

[2] Barbara A. Kitchenham, Shari Lawrence Pfleeger, Lesley M. Pickard, Peter W. Jones, David C. Hoaglin, Khaled El Emam, and Jarrett Rosenberg. Preliminary guidelines for empirical research in software engineering. *IEEE Transactions on Software Engineering*, 28(8):721–734, August 2002.

[3] David L. Parnas and Bill Curtis. Empirical research in software engineering: A critical view. *IEEE Software*, 26(6):56–59, November–December 2009. doi:10.1109/MS.2009.184.