File 20110610.0909: Notes from meeting with Dr Martin:

I discussed chapter two with Dr Martin in our meeting Friday. It was not as far along as the first chapter because the grounded theory methodology is not something I have spent years thinking about. As far as the content, I lack a rationale for the methodology. Why choose these three case studies? Why three, not more or fewer? Pragmatically, these three are the data I had available, and pragmatically, grounded theory is suitable for understanding data where the researcher cannot choose the data or its format, and where the quality of data collected might be highly variable from case to case. I need a stronger scientific reason for choosing three case studies, these particular case studies, and the GTM. Also, the organisation of the chapter is wrong.

I felt last night like I was blowing smoke at the reader, not providing a scientifically justifiable argument. Dr Martin suggested a three-part organisation for the chapter. Part I is the conjecture. Part II is the scaffolding for proving the conjecture. Part III is the justification for the scaffolding. I need t clearly communicate a stronger scientific reason for choosing this methodology, and justify it at every step along the way.

Show how this approach matches your thesis.

Dr Martin said he was confused about the purpose of this chapter. I said it was to introduce the three case studies, tell the specialised methodology required for each one, since they are different, and to argue for the suitability of grounded theory to solve it. The results of each case study will be in a separate chapter of its own.

I promised to give a new version, longer and better organised, to Dr Martin by Wednesday, my new deadline. GSS reports are due next week, and this way I can report six formal meetings this term and two completed chapters in the GSS report.

I looked in the grey book of regulations for guidance on formatting a dissertation in Oxford style. There is little guidance. When Dr Martin did his, he spent many happy hours tweaking his format to get things like drop caps. When Dr Martin is Senior Proctor, he is going to revert the regulations to the old wording, which is that a properly formatted dissertation should feel like a well designed book, and leave it at that. I said I expect to see that in Congregation [note: I should have said Council] in the *Gazette* some day. We discussed double spacing, which Dr Martin dislikes very much. The reason for double spacing in typescript was to allow minor revisions to be made by rolling the paper back into a typewriter and typing between the lines. I never knew that. We decided after all to keep the double spacing, as it provides a useful clue to the length of chapters, around ten pages, and the overall length of the dissertation, around 150 pages. Double spacing wastes paper, Dr Martin says, but it's traditional and expected by some external examiners, so do it. Dr Martin prefers that the formatting feel like an especially well designed book. That's why he likes to see drop caps.

There is no University-wide LaTeX document class file, and no departmental one either. The closest thing I could find was an example from the History department, which I followed for its margin width and double spacing and type size guidance. I made the mistake of upgrading MikTeX from 2.7 to 2.9 the other day, which broke everything, just to get double spacing. I should never have done that. Dr Martin thinks LaTeX really ought to auto-configure itself by now. It should be a grand challenge in computer science.

I thought today's was a particularly productive meeting, judging at least from the amount of notes I am tying up afterwards.

We talked about RSA SecurID and the recent compromise, HSBC and Barclay's bank security tokens, and a recent court case in Maine where a U.S. District Court judge dismissed responsibility by Ocean Bank for $300,000 stolen when thieves installed spying software on the bank customer's computer and stole his passwords. The judge ruled that as far as the bank could tell, it had received valid authentication before transferring the money. We talked about D-Wave Systems' 128-qbit adiabatic quantum computer and DARPA's mission, 'the prevention and the creation of strategic surprise'.

Dr Martin encouraged me to take lots of photos if I take apart the old SecurID token. Look for a crypto fill port. Look for evidence that it stops working if tampered with.

On the GCHQ and CC story related by Prof. Anderson, try to find a source for it in his published papers. Dr Martin thinks it might be an old story, since the Chip & PIN work was done years ago. I hadn't heard the story about the CC certificates before; I think it might be in Prof. Anderson's WEIS paper he's giving next week. Track down this reference. Was the claimed CC evaluation at EAL4? I would think a FIPS 140-2 level 4 cryptographic module validation would be more suitable. If it wasn't originally level 4 tamper resistance, after lightbluetouchpaper's attack it should be now.

Dr Martin is at the Trusted Computing conference in Germany next week. We have a tentative meeting scheduled for Wednesday, 15th June 2011 at 5pm German time, 4pm UK time, 9am Mountain daylight time. I should try calling Dr Martin on Skype; if he is not on-line, then something happened.

It was an infodump today.

References