File 20110715.0845: Notes from meeting with Dr Martin:

Prof. Creese (pron. like 'crease') is the heavyweight; Michael Goldsmith came along with her as a buy one get one free deal from Warwick. He is funded off one of her grants. The Professor of Cyber Security did not have to go through Council because while she has the title of professor, it's not a named chair. So it didn't appear in the *Gazette*. The University has many ways of accomplishing things. There was some controversy over the title; Dr Martin wonders how cool that title will sound ten years from now. But who plans ten yours out in this field?

Regarding blog postings, Dr Martin writes well and prolificly. He said he thought the writing was rough. I said he ought to write it for publication. Regarding the post on disk erasure, when I got to the end, a comment would have been superfluous because I couldn't think of anything he had not already said. He covered shredding, data transfer rates on the interface, encryption and warehousing, which is two more aspects than every other article I've read on the subject.

Regarding data retention, you don't always get to choose what PII you have on your network.

Regarding the 'Defence Science: Trustworthy Systems call' email dated 14th July 2011, we discussed sending these guys a proposal. I described the success I had sending DARPA, AFRL, ARL and NRL proposals that started out, 'This is a risky approach…we think it will work, and here's why, but it's risky and it might not work at all.' I told Dr Martin that the AFRL people said ours was unique amongst the proposals they received, and very different from the proposals they got from commercial companies. Dr Martin has long wanted to look at the question of whether historical data on breaches, together with the CVE, could be used to predict future atacks on areas elsewhere in the CVE. Dr Fléchais, when he heard about the idea, again brought up the Common Criteria, but Dr Martin (and I agree) it needs to be more empirical than the CC. I wondered aloud what analytical techniques exist for predicting from historical data; all I could think of off-hand was Bayesian reasoning, but all I know of that is from a philosophical perspective, except that it has recently and successfully been applied to spam filtering. I think that an application of Bayesian reasoning, as distinct from Bayesian analysis, might be the key to cracking the CVE prediction problem. What other data sources besides CVE are available? I suggested Anonymous, Wikileaks, the California laws requiring notification of breaches, DoD reports on memory sticks scattered in car parks, all the open sources analysis that had been done by individuals on Stuxnet, and perhaps information leaked out of Anonymous suggesting how many attempts they may have made before they successfully got in. The defender has to be right every time; the attacker only has to be right once. Would Anonymous announce, possibly out of boasting, how many things they tried before they got in? I don't think I can use the BYZANTINE HADES report, but there may be open sources that we could correlate. Dr Martin says he is surprised no one has ever published this sort of research before. I offered help writing and labour if he wants to send MOD a proposal. Would I be treated as a foreign national? Perhaps, but he thought LM UK was there.

Submission deadline for the Defence Science: Trustworthy Systems call is mid September. I think we should make the proposal before somebody else does.

We talked about CAPPS II and how it nearly induced me to quit the company, if Congress hadn't shut them down (again, and again) after the announcement I read in the *Federal Register*. I still have strong feelings about that system. LM got sued by DHS over the PNR data that DHS had provided LM after LM eagerly stepped up to build CAPPS II, and later Total Information Awareness, and whatever it's called now that the system is undoubtedly in production. At least the system in production is not Radiant Trust Gold. I would have quit the company over that invasion of privacy. Funny that I still work for a company that builds ICBMs, in addition to Mars rovers and other cool things.

The Defence Science: Trustworthy Systems call people are keen on accreditation of COTS products. I mentioned my Plan B of applying this research to certification and accreditation of COTS products if America ever stops getting involved in land wars in Asia. If perchance they do, and my funding source at present disappears, I don't think the attacks by Anonymous on health care, banks, and other unclassified organisations will cease. My research is applicable there.

When is my next written work due? I think I put September 15th in the Application, but I am aiming for submission of written work for the assessors' consideration by 15th August. That gives them a couple weeks to look it over. Dr Martin is on holiday the first three weeks of August, but back the fourth week of August and his schedule the first week of September is completely open. I am tentatively planning a trip to Oxford the first week of September. Have to get the Assessors on board soon if so.

Advice: finish Chapter 2. Move the analysis into Chapter 3 if necessary, but don't over-think the methodology. The assessors are going to want to talk specifics on grounded theory methodology, so be able to show how you do the coding, classification, memo writing, and refinement of the grounded theory. Have a grounded theory of what developed over the course of the R'' certification calls. Show how it is grounded in the data, and how you found it and refined it over time.

Dr Martin said it would be okay to write Chapter 3 first, then go back to Chapter 2.

For the assessors, give them something that looks like a thesis, but with placeholders where some chapters are.

Call ended 0830-something. Next meeting Friday, 22nd July at 0800 my time, 1500 Oxford time.

References